Univerzita Karlova v Praze
Právnická fakulta

Pavel Vyškovský

e-Government

Diplomová práce

Vedoucí diplomové práce: Mgr. František Korbel, Ph.D.

Katedra: Správního práva a správní vědy

Datum vypracování práce (uzavření rukopisu): 23. 10. 2014

Čestné prohlášení:

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, všechny použité prameny a literatura byly řádně citovány a práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 23. 10. 2014 Podpis

Poděkování:

Rád bych poděkoval Mgr. Františku Korbelovi, Ph.D., vedoucímu diplomové práce, za poskytnutí podkladů a za vstřícnost a připomínky při zpracování diplomové práce.

OBSAH

Úvod

Odborná a nestranná služba veřejnosti, spolu s efektivností a transparentností, patří k základním požadavkům doktríny nazývané dobrá správa *(Good Administration, či Good Governance, někdy též Good Government).*[1] Právo občana na dobrou správu je institutem rozvinutým jak v dokumentech Rady Evropy, tak v právu Evropské unie. Nejnovějším aktem vydaným Radou Evropy, s cílem definovat základní právo na dobrou veřejnou správu, je Doporučení Rec(2007)7 Výboru ministrů členským zemím o dobré veřejné správě/good governance, které bylo přijato 20. 6. 2007. V právu Evropské unie jsou pak základními dokumenty Listina základních práv Evropské unie a Evropský kodex dobré správní praxe.

V České republice byl pojem dobrá správa blíže specifikován základními principy, které v roce 2006 stanovil veřejný ochránce práv, JUDr. Otakar Motejl. Mezi tyto principy, mimo povinnosti dodržovat právní řád, být nestranný při výkonu veřejné správy, rozhodovat včasně, předvídatelně, přesvědčivě, přiměřeně a odpovědně, byly zařazeny i principy součinnosti a otevřenosti. Podle principu součinnosti *„je nutné po osobách vyžadovat pouze takovou míru součinnosti, která je k dosažení účelu nezbytná. Rovněž je třeba o tomto principu uvažovat i ve vztazích mezi úřady. Každý úřad má v případě potřeby udržovat kontakty s jinými úřady, případně zajistí vzájemnou komunikaci mezi svými vlastními odbory či organizačními jednotkami.“*[2] Podle principu otevřenosti pak každý *„úřad umožní osobám nahlížet do všech úředních dokumentů a pořizovat si jejich kopie. Úřad pečlivě dodržuje spisový pořádek a vede záznamy o příchozí a odchozí poště, takže je schopen jednotlivé dokumenty vyhledat.“*[3]

Veřejná správa při obrovském objemu činností, které v moderních demokratických státech vykonává, může být účinná a efektivní pouze při správném zapojení a využívání informačních a komunikačních technologií. V době neustále se rozvíjejících informačních technologiích je tak nutné činnost veřejné správy neustále přizpůsobovat oprávněným požadavkům společnosti na snadnou dostupnost veřejné správy, na její efektivnost a na informovanost o jejich činnostech.

[1] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2. vydání. Leges, 2012. s 83
[2] POMAHAČ, Richard. *Základy teorie veřejné správy*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. s 159
[3] POMAHAČ, Richard. *Základy teorie veřejné správy*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. s 159

Využívání informačních technologií při výkonu veřejné správy bývá mezinárodně označováno jako eGovernment a jeho účelem je právě přispět k doktríně dobré správy. Veřejná správa se však ve vyspělých státech musí řídit principem legality, který je v České republice zakotven v čl. 2 odst. 3 ústavního zákona č. 1/1993 Sb., Ústava České republiky (dále jen „Ústava“). Rychlý rozvoj moderní společnosti a komunikačních technologií tedy vyžaduje adekvátně rychlou reakci veřejné správy při poskytování služeb, a ta zase očekává rychlou reakci legislativy, která jí umožní své poslání naplňovat.

Téma diplomové práce jsem si zvolil z důvodu zájmu o problematiku legislativního vymezení eGovernmentu v České republice a následným porovnáním dané právní úpravy se současnou aplikační praxí v České republice. Rád bych poukázal na rozdíly mezi někdy značně teoretickými a obecnými koncepty zdůvodňujícími nezbytnou potřebu zavádění elektronizace veřejné správy, které by měly usnadnit přístup veřejnosti k veřejné moci a prostřednictvím elektronických institutů se na ní podílet a kontrolovat ji, a mezi skutečnou a složitou každodenní praxí při fungování orgánů veřejné moci. Jelikož se jedná o oblast velice širokou, jak rozsahem, tak obsahem, zahrnující v nejširším smyslu vše od tzv. e-demokracie, která přes e-participaci umožňuje občanům podílet se na správě věcí veřejných, až po jednotlivé specifické služby eGovernmentu, kterými jsou v České republice např. datové schránky či základní registry veřejné správy, zaměřuji se na komplexní popis současného stavu praxe v důležité části eGovernmentu, v tzv. eJustici. Tuto oblast jsem si vybral zejména proto, že je mi známa jak z mé praxe u soudu, tak ze současného působení na Ministerstvu spravedlnosti ČR, kde se elektronizaci justice věnuji. Rovněž se v této oblasti dá názorně popsat každodenní praxe fungování eGovernmentu v České republice.

Cílem mé diplomové práce je porovnat teoretické koncepty odůvodňující zavedení a rozvoj eGovernmentu, se skutečným dosaženým stavem, a to zejména v oblasti justice. Otázky elektronizace justice jsou úzce spojeny s naprostou většinou obecných institutů eGovernmentu v České republice, proto se v diplomové práci pokusím zdůraznit jejich vzájemné propojení, a to jak po legislativní, tak i faktické stránce.

Svou diplomovou práci jsem rozdělil do čtyř částí. První část vymezuje pojem eGovernmentu, jeho historii, legislativní a institucionální zajištění. Druhá část stručně popisuje současné a v praxi již zavedené nejdůležitějších části elektronizace veřejné správy v České republice. Třetí část je pak věnována popisu stávající praxe a fungování jednotlivých částí

eGovernmentu v oblasti justice. Ve čtvrté části se upozorňuji na problémy, které s sebou může elektronizace veřejné správy přinášet.

1. Teorie e-Governmentu

1.1 Pojem eGovernmentu a jeho členění

Definice pojmu eGovernment, stejně jako pojmu dobrá správa, není v české legislativě v současné době vymezena. Ani právní teorie se neshodne na jednoznačném vymezení. Existují definice obecnější i popisnější. Někteří autoři vymezují daný pojem široce jako „*efektivní a výkonné služby a informační a komunikační technologie umožňující občanům se plně podílet na životě společensky a kulturně tvůrčích komunit včetně demokratického procesu.*“[4] Evropská komise v dokumentu s názvem eGovernment-Action Plan 2011-2015 z roku 2011 vymezuje e-Government „*jako použití nástrojů a systémů, které jsou zde díky informačním a komunikačním technologiím, pro poskytování lepších veřejných služeb občanům a podnikům.“*[5] Ani Ministerstvo vnitra ČR, do jehož kompetence rozvoj eGovernmentu patří, jasnou definici nenabízí. Pokus o takové definování lze nalézt v jediném dokumentu zveřejněném na internetových stránkách Ministerstva vnitra. Dle tohoto eGovernment představuje „*transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních technologií s cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům.“*[6]

U všech těchto definic lze nalézt společné znaky vymezující hlavní smysl eGovernmentu. Je jím cíl poskytovat lepší služby veřejnosti a občanům prostřednictvím informačních technologií a umožnit jim podílet se na správě věcí veřejných a tím posílit demokratizaci veřejné správy. Může tak jít o e-participaci v nejširším slova smyslu, jako je možnost volit zastupitele v elektronických volbách (e-voting), tak možnost elektronických referend či elektronických petic. V neposlední řadě může jít o různá, více či méně oficiální, internetová diskusní fóra pro e-participaci či možnost klást elektronickou cestou dotazy úřadům a voleným zástupcům. Tyto cíle jsou těmi základními, odpovídajícími požadavkům na dobrou správu.

[4] SMEJKAL, Vladimír a Michal Altair VALÁŠEK. *Jak na datové schránky: praktický manuál pro každého*. Praha: Linde, 2012. s 25
[5] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2. vydání. Leges, 2012. s 38
[6] MINISTERSTVO VNITRA. *Indikátory Prioritní osy 1a,1b: Oblasti intervence: 1.1A, 1.1B - Rozvoj informační společnosti ve veřejné správě* [online]. [cit. 2013-12-12]. Dostupné z: www.mvcr.cz/soubor/indikatory-prioritnich-os-1a-a-1b-pdf.aspx

Mezi neméně významné důvody rozvoje eGovernmentu lze zařadit i snahu o efektivní fungování veřejné správy, a to jak státní správy, tak i samosprávy. Jde hlavně o snížení byrokratické zátěže pro veřejnost a podnikatele, o odstranění povinnosti dávat různým orgánům opakovaně stejné údaje, dále o možnost komunikovat s veřejnými orgány elektronickou cestou, tedy bez nákladů na dojíždění a čas. Dalším důležitým cílem je možnost kontroly transparentnosti rozhodování veřejné správy prostřednictvím tzv. otevřených dat, s čímž souvisí i možnosti omezení často zmiňovaného korupčního jednání. Nelze opomenout ani další ekonomický aspekt, kterým je uplatnění soukromého sektoru a jeho pracovníků, kteří se na rozvoji eGovernmentu, dle zadání orgánů veřejné moci, podílejí.

Na straně orgánů veřejné moci jde o personální, materiální a finanční úspory při výkonu činnosti veřejné správy. Konkrétně může jít o hromadné zpracovávání standardizovaných elektronických žádostí a o automatizaci rutinních činností, což může vést ke snížení počtu zaměstnanců orgánů veřejné správy. Dále jde o možnost dálkového přístupu do sdílených elektronických databází, které orgán veřejné moci využívá při své činnosti. S tím úzce souvisí zvýšení rychlosti rozhodování.

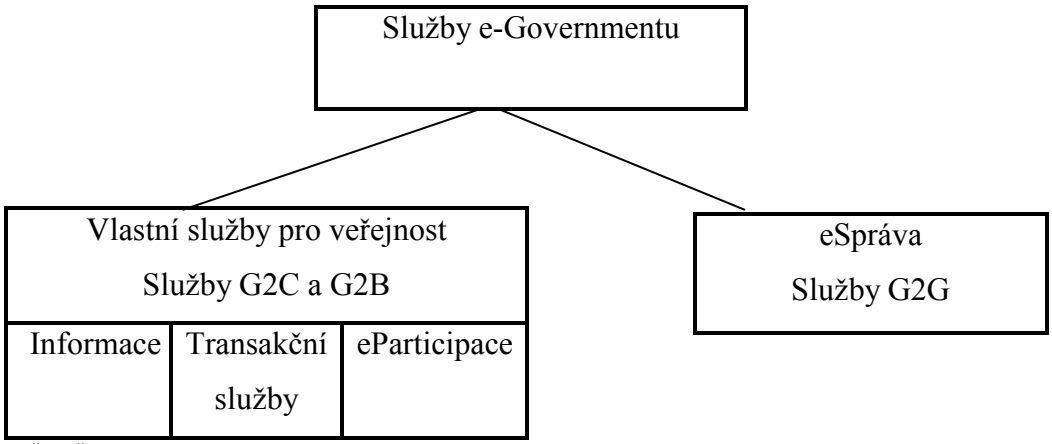
Co se týče rozsahu pojmu eGovernment z hlediska státní moci, lze konstatovat, že jej lze vztáhnout na všechny orgány veřejné moci. Pojem orgány veřejné moci používá např. čl. 87 odst. 1 písm. d) Ústavy, aniž by jej blíže definoval. Veřejnou mocí se pak rozumí taková moc, která *„autoritativně rozhoduje o právech a povinnostech subjektů, ať již přímo, nebo zprostředkovaně.“*[7] Mezi orgány veřejné moci tak můžeme zařadit jak orgány státní správy či soudní moci, tak orgány územní samosprávy.

I eGovernment lze členit podle různých kritérií. Nejčastěji se pro popis jednotlivých částí používají zkratky G2C (Government-to-Citizen), G2B (Government-to-Business) a G2G (Government-to-Government).

Členění služeb e-Governemtu lze tedy rozdělit takto:

[7] HENDRYCH, Dušan. *Správní právo: obecná část*. 7. vyd. Praha: C.H. Beck, 2009, xxxviii, 837 s. Právnické učebnice (C.H. Beck). s. 119

Obrázek č. 1: Členění eGovernmentu



Pramen: ŠPAČEK, David. Kategorie služeb e-governmentu, EGovernment: cíle, trendy a přístupy k jeho hodnocení. Vyd. 1. V Praze: C.H. Beck, 2012, xix, s 6

1.2 Historie vývoje e-Governmentu v České republice

Pro historii rozvoje e-Governmentu v České republice byla v první dekádě po roce 1989 typická absence jednotné koncepce a silného veřejného orgánu, který by za rozvoj odpovídal. První počátky pokusů lze spatřovat ve vzniku Komise vlády pro státní informační systémy v roce 1991, která měla „*zajistit odstranění roztříštěnosti informačních systémů a koordinovat rozvoj jednotného státního informačního systému*.“[8] Za další významnější událost na poli zavedení e-Governmentu lze zřejmě považovat vznik, dnes již neexistujícího Úřadu pro státní informační systém, který byl k 1. 11. 1996 zřízen zákonem č. 272/1996 Sb., aniž by mu byla stanovena oblast jeho působnosti. V roce 1998 pak byla zřízena Rada vlády pro informační politiku, která, spolu s Úřadem pro státní informační systémy, předložila v roce 1999 první českou koncepci rozvoje e-Governmentu s názvem Státní informační politika – cesta k informační společnosti. Tuto koncepci schválila vláda v roce 1999. Bylo stanoveno osm prioritních oblastí, a to informační gramotnost, informatizovaná demokracie, rozvoj informačních systémů veřejné správy, komunikační infrastrukturu, důvěryhodnost a bezpečnost informačních systémů a ochrana osobních dat, elektronický obchod, transparentní ekonomické prostředí a vytvoření stabilní a bezpečné informační společnosti. Zároveň byly stanoveny základy postupu realizace této politiky, která počítala s tím, že zmíněná Rada pro

[8] ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. Vyd. 1. V Praze: C.H. Beck, 2012, xix, s 53

vládní informační politiku spolu s Úřadem pro státní informační systém připraví Akční plán státní informační politiky. Akční plán byl schválen v roce 2000.

Za významné milníky v dané oblasti lze považovat nabytí účinnosti dvou zákonů v roce 2000. Dne 1. 10. 2000 nabyl účinnosti zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), čímž byl učiněn první větší krok k zavedení eGovernmentu. Teprve tímto zákonem došlo k vymezení pojmů elektronický podpis, datová zpráva, akreditovaný poskytovatel certifikačních služeb, atd. Tento zákon měl velký dopad i na činnost veřejné správy a justice, protože stanovil povinnost orgánům veřejné správy přijímat podání v elektronické podobě podepsaná elektronickým podpisem. Došlo tak k zavedení elektronických podatelen, a to všemi orgány veřejné moci, na které se procesní předpisy vztahovaly. Tato povinnost byla později upřesněna vyhláškou č. 496/2004 Sb., o elektronických podatelnách.

V roce 2000 rovněž nabyl účinnosti zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „zákon o ISVS“). Tímto zákonem byl zřízen Úřad pro veřejné informační systémy, jakožto nástupce Úřadu pro státní informační systém, a v ust. § 4 odst. 2 a 3 mu již byly dány rozsáhle kompetence v oblasti státních informačních systémů.

Existence Úřadu pro veřejné informační systémy však neměla dlouhého trvání. K 1. 1. 2003 přešly jeho kompetence na nově zřízené Ministerstvo informatiky, které bylo zřízeno zákonem č. 517/2002 Sb. Podle nového ust. § 18 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky (kompetenční zákon) bylo Ministerstvo informatiky „*ústředním orgánem státní správy pro informační a komunikační technologie, pro telekomunikace a poštovní služby*.“[9] Rovněž došlo k novelizaci zákona o ISVS, kterým byly veškeré dosavadní kompetence Úřadu pro státní informační systém přesunuty na nové ministerstvo. V oblasti eGovernmentu byla vypracována a v roce 2003 představena nová Státní informační a komunikační politika přezdívaná e-Česko 2006. Tato byla schválena vládou v roce 2004. Z konkrétních kroků Ministerstva informatiky lze uvést spuštění Portálu veřejné správy v září 2003. Ministerstvo informatiky realizovalo rozsáhlou legislativní činnost, a to jak v oblasti přípravy návrhů zákonů (např. návrh zákona o

[9] Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky

sdílení dat ve veřejné správě, návrh zákona o elektronických komunikacích, návrh zákona o e-Governmentu, atd.), tak i v oblasti vydávání podzákonných předpisů.

K další velké změně došlo v oblasti eGovernmentu v České republice v roce 2006, kdy zákonem č. 110/2007 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů došlo s účinností od 1. 6. 2007 ke zrušení Ministerstva informatiky a většina jeho kompetencí v oblasti e-Governmentu přešla na Ministerstvo vnitra ČR. Nové cíle byly stanoveny zejména ve strategii s názvem „Efektivní veřejná správa a přátelské veřejné služby – Strategie realizace Smart Administration v období 2007 – 2015“, která byla později specifikována dokumenty „Strategie rozvoje služeb pro informační společnost“ a „Strategií implementace e-Governemntu v území.“ Tato strategie byla schválena vládou a implementace hlavních úkolů byla svěřena právě Ministerstvu vnitra.

Na základě této strategie došlo k největším legislativním změnám od roku 2000, a to k přijetí průlomového zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, který nabyl účinnosti k 1. 7. 2009 (někdy nazývaného jako zákon o e-Governmentu) a k přijetí zákona č. 111/2009 Sb., o základních registrech, který nabyl účinnosti k 1. 7. 2012.

1.3 Základní strategické rámce e-Governmentu v Evropské unii a v České republice

V Evropské unii jsou strategické dokumenty popisující další směr v rozvoji e-Governmentu obsaženy ve strategiích označených jako eEurope. V roce 2000 byl Evropskou komisí předložen Radě dokument s názvem „eEurope – An Information Society For All“, který byl následně schválen v podobě akčního plánu eEurope 2002. Dle akčního plánu měly členské státy ve spolupráci s Evropskou unií „*kromě online zpřístupnění základních dat, zjednodušení administrativních procedur pro podnikatelské subjekty či koordinování do konce roku 2002/3 zajistit všeobecný elektronický přístup ke službám, které byly prohlášeny za základní.“*[10] Mezi tyto základní služby patří např. možnost podat elektronickou cestou přiznání daně z příjmu elektronicky, žádat o osobní dokumenty (pasy a řidičské průkazy), o stavební

[10] ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. Vyd. 1. V Praze: C.H. Beck, 2012, xix, s 24

povolení, oznámení na policii, atd. Po tomto dokumentu následovaly další strategické plány, např. eEurope 2005 z roku 2002 a následně v roce 2005 přijala Evropská komise nový strategický dokument i2010, ze kterého vznikl akční plán i2010 eGovernment Action Plan. Zatím posledním akčním plánem je The European eGovernment Action Plan 2011 - 2015 z roku 2010, který si klade za cíle „*zvýšení schopností uživatelů, zajištění snadného přístupu k informacím a průhlednosti a umožnění účinného zapojení občanů a podnikatelských subjektů do tvorby politiky.*“[11] Dále členské státy „*nabídnou do roku 2015 občanům přeshraniční e-služby, které jim umožní studovat, pracovat, bydlet, obdržet zdravotnickou péči či jít do důchodu kdekoliv v EU.*“[12]

V České republice je nejvýznamnější strategií v oblasti eGovernmentu již zmíněný dokument s názvem „Efektivní veřejná správa a přátelské veřejné služby – Strategie realizace Smart Administration v období 2007 – 2015“. Jako globální cíl je zde označeno „*zefektivnění fungování veřejné správy a veřejných služeb, podpořit socioekonomický růst ČR a zvýšit kvalitu života občanů.*“[13]

Mezi konkrétnější strategické cíle řadí strategie např. cíl „*zlepšit a zjednodušit regulatorní prostředí a vytvořit atraktivní prostředí pro podnikatele, domácí i zahraniční investory, zefektivnit činnost úřadů veřejné správy, snížit finanční nároky na chod administrativy a zajistit transparentní výkon veřejné správy. Vytvořit centrální registry veřejné správy tak, aby bylo možné bezpečné sdílení dat orgány veřejné moci a zároveň byl občanům umožněn oprávněný přístup k údajům vedeným v těchto registrech. Důsledně prosazovat preventivní i represivní opatření v boji s korupcí, prosazovat e-Government s důrazem na bezpečný a jednoduchý přístup k veřejným službám prostřednictvím sítě internetu, připravit právní úpravu, která zajistí elektronizaci procesních úkonů ve veřejné správě, zrovnoprávnit formu listinnou s formou elektronickou, umožnit bezpečnou komunikaci mezi úřady a veřejností a optimalizovat interní procesy veřejné správy s využitím informačních komunikačních technologií. Dále vybudovat síť kontaktních míst veřejné správy, univerzálního místa pro fyzické a právnické osoby, kde bude možné z jednoho místa činit veškerá podání vůči orgánům veřejné správy, získávat veškeré ověřené údaje vedené v dostupných centrálních registrech a*

[11] ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. Vyd. 1. V Praze: C.H. Beck, 2012, xix, s 27
[12] ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. Vyd. 1. V Praze: C.H. Beck, 2012, xix, s 28
[13] MINISTERSTVO VNITRA. *Efektivní veřejná správa a přátelské veřejné služby: Strategie realizace Smart Administration v období 2007 - 2015* [online]. 2007. vyd. 2007 [cit. 2013-12-19]. Dostupné z: www.mvcr.cz/soubor/modernizace-dokumenty-strategie-pdf.aspx

evidencích a získávat informace o průběhu všech řízení, která jsou s danou osobou či o jejích právech a povinnostech orgány veřejné moci vedena.“[14]

V oblasti justice se klade za cíl „*zavést systém elektronické justice, včetně dokončení všech návazných projektů vedoucích k zefektivnění práce justice a zlepšení komunikace justice jak s odbornou, tak i laickou veřejností.“* [15]

Z této strategie vychází zatím poslední dokument označený jako „Strategický rámec rozvoje eGovernmentu 2014+“, který vydalo v roce 2008 Ministerstvo vnitra, a který byl opět schválen usnesením vlády.

1.4 Současná právní úprava e-Governmentu v České republice

Současná právní úpravu e-Goverenmentu se opírá o několik stěžejních zákonů a značné množství podzákonných doprovodných předpisů.

Základní normou nejvyšší právní síly stanovující rozsah působnosti veřejné moci a tím rozsah eGoverenmentu je Ústava České republiky, která ve svém čl. 2 odst. 3 stanovuje zásadu legality, podle které může být státní moc uplatňována je v případech, v mezích a způsoby, které stanoví zákon.

Dalším důležitým ustanovením je článek 17 usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších předpisů (dále jen „Listina“), která jako jedno z politických práv uvádí právo na informace, neboť „*aktivní účast jednotlivců na životě státu vyžaduje mimo jiné dostatečnou sumu informací.“*[16]

[14] MINISTERSTVO VNITRA. *Efektivní veřejná správa a přátelské veřejné služby: Strategie realizace Smart Administration v období 2007 - 2015* [online]. 2007. vyd. 2007 [cit. 2013-12-19]. Dostupné z: www.mvcr.cz/soubor/modernizace-dokumenty-strategie-pdf.aspx

[15] MINISTERSTVO VNITRA. *Efektivní veřejná správa a přátelské veřejné služby: Strategie realizace Smart Administration v období 2007 - 2015* [online]. 2007. vyd. 2007 [cit. 2013-12-19]. Dostupné z: www.mvcr.cz/soubor/modernizace-dokumenty-strategie-pdf.aspx

[16] PAVLÍČEK, Václav. *Ústavní právo a státověda*. Praha: Linde, 2004, s. 139

Elektronizaci orgánů veřejné moci však musí předcházet posouzení, zda jejím provedením nedojde k zásahu do základních právních principů či základních práv a svobod. Proto by každému zásahu měl předcházet test proporcionality, tak, jak jej vymezil Ústavní soud v nálezu pod spisovou značkou Pl. ÚS 24/10, dle kterého „*posouzení přípustnosti daného zásahu z hlediska zásady proporcionality (v širším smyslu) zahrnuje tři kritéria. Prvním z nich je posouzení způsobilosti naplnění účelu (nebo také vhodnosti), přičemž je zjišťováno, zda je konkrétní opatření vůbec schopno dosáhnout zamýšleného cíle, jímž je ochrana jiného základního práva nebo veřejného statku. Dále se pak jedná o posouzení potřebnosti, v němž je zkoumáno, zda byl při výběru prostředků použit ten prostředek, který je k základnímu právu nejšetrnější. A konečně je zkoumána přiměřenost (v užším smyslu), tj. zda újma na základním právu není nepřiměřená ve vazbě na zamýšlený cíl, tzn., že opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky převyšovat pozitiva, která představuje veřejný zájem na těchto opatřeních.*“

Mezi stěžejní zákonné normy spadající do oblasti správního práva hmotného i procesního a upravující současný rozsah eGovernmentu v České republice, včetně jejich nejdůležitějších prováděcích předpisů, lze zařadit:

1. zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (dále jen „zákon o archivnictví“),
2. zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „zákon o ISVS“),
3. zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (dále jen „zákon o elektronickém podpisu“),
4. zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (dále jen „zákon o DS“),
5. zákon č. 111/2009 Sb., o základních registrech (dále jen „zákon o ZR“),
6. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím,
7. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů,
8. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

Podrobný výčet zákonných a na ně navazujících podzákonných přepisů je uveden v příloze č. 1.

Tyto základní právní předpisy v oblasti eGovernmentu měly a mají rovněž dopad na velké množství jiných právních předpisů, které byly novelizovány tak, aby byly s těmito zákony v souladu. Jako příklad lze uvést jak nejdůležitější procesní předpisy pro oblast justice, kterými jsou zákon č. 99/1963 Sb., občanský soudní řád (dále jen „o.s.ř."), zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád) (dále jen „trestní řád"), zákon č. 150/2002 Sb., soudní řád správní a zákon č. 500/2004 Sb., správní řád, tak i velkou řadu jiných předpisů, např. zákon č. 325/1999 Sb., o azylu, zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky, zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech, zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů, zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), zákon č. 85/1996 Sb., o advokacii a další.

1.5 Institucionální zajišťování rozvoje e-Governmentu v České republice

Ministerstvo vnitra ČR je v souladu s ust. § 12 odst. 1 písm. o) zákona č. 1/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ústředním orgánem státní správy v oblasti informačních systémů státní správy. Podle písm. n) téhož ust. pak rovněž v oblasti elektronického podpisu. Podle odst. 6 pak Ministerstvo vnitra ČR plní koordinační úlohu pro informační a komunikační technologie.

Další působnost Ministerstva vnitra ČR je dána a blíže specifikována zvláštními zákony. Jde např. o ust. § 4 zákona o ISVS, dle kterého ministerstvo vykonává téměř veškerou správu v oblasti informačních systémů veřejné správy. Dle tohoto ustanovení např. „*zpracovává návrhy strategických dokumentů v oblasti informačních systémů veřejné správy, a to i z hlediska bezpečnosti těchto systémů, a předkládá tyto dokumenty vládě, sleduje a analyzuje informační potřeby veřejné správy a stav informačních systémů veřejné správy, připravuje nebo koordinuje přípravu záměrů pro budování nebo přetváření informačních systémů veřejné správy vyvolané, zajišťuje tvorbu metodických pokynů pro výkon odborných činností spojených s vytvářením, rozvojem a využíváním informačních systémů veřejné správy, vytváří a spravuje veřejný informační systém, který obsahuje základní informace o dostupnosti a*

obsahu zpřístupněných informačních systémů veřejné správy, koordinuje a vytváří podmínky pro činnost kontaktních míst veřejné správy.“ Dále kontroluje u orgánů veřejné správy dodržování povinností stanovených zákonem o ISVS, vykonává působnost v oblasti akreditace a atestací informačních systémů veřejné správy či prostřednictvím portálu veřejné správy vydává Věstník, v němž uveřejňuje metodické pokyny.

Dalším zákonem, který vymezuje působnost Ministerstva vnitra ČR je zákon o elektronickém podpisu, kdy podle ust. § 9 ministerstvo vnitra uděluje a odnímá akreditaci poskytovatelům certifikačních služeb na území České republiky, vede jejich seznam a ten zveřejňuje. Dále udržuje seznam důvěryhodných certifikačních autorit dle evropských přepisů, a to dle směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy v některém ze členských států EU a Rozhodnutí komise 2009/767/ES, kterým se stanoví opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“, podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu. Zákon dále stanoví povinnosti poskytovatelům certifikačních služeb poskytovat ministerstvu informace, umožnit mu přístup do prostorů a poskytovat mu na vyžádání veškerou dokumentaci.

Rovněž zákon o DS dává veškerou působnost v oblasti datových schránek a autorizované konverze právě Ministerstvu vnitra ČR. Podle ust. § 2 odst. 2 zákona o DS „*datové schránky zřizuje a spravuje Ministerstvo vnitra.“* Dle dalších ustanovení zákona pak ministerstvo zpřístupňuje, znepřístupňuje a zrušuje datové schránky v souladu se zákonem. Ministerstvo je správcem informačního systému datových schránek a vykonává další působnost v souladu se zákonem o DS. Zákon o ZR pak vytvořil Správu základních registrů, jakožto správní úřad podřízený Ministerstvu vnitra ČR, který je správcem informačního systému základních registrů (dále jen „ISZR“) a zajišťuje jeho provoz a další činnosti stanovené zákonem.

To však neznamená, že všechny informační systémy orgánů veřejné moci jsou spravovány výlučně Ministerstvem vnitra ČR. Jednotlivé orgány státní správy a samosprávy vykonávají vlastní správu informačních systémů, které potřebují pro výkon své činnosti nebo činnosti organizací v jejich působnosti, a to v souladu se zákony, které jim takováto oprávnění dávají. Ministerstvo vnitra ČR pak tuto činnost zastřešuje a udává hlavní směry rozvoje informačních technologií a systémů jako celku.

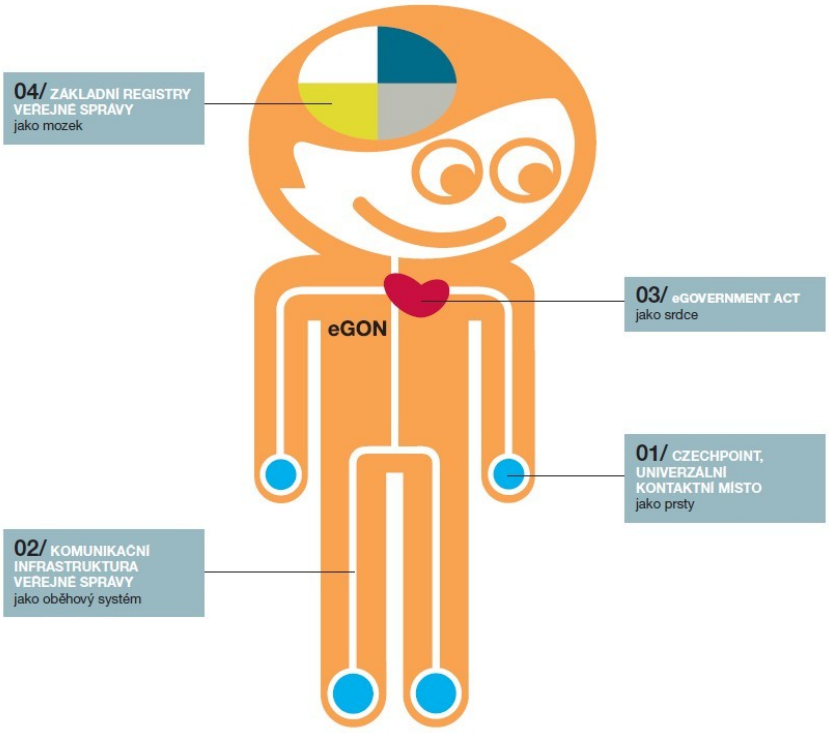
1.6 Shrnutí kapitoly

Vývoj e-Governmentu nebyl, a stále není, v České republice vůbec jednoduchý. Vyznačuje se nekoncepčností a neustálými změnami v působnosti státních orgánů, které by měly jeho rozvoj organizovat a vést. Právní úprava je dle mého názoru zbytečně roztříštěná v množství právních předpisů, které navíc netvoří jeden vzájemně propojený a související celek. Každý zákon upravuje určitou oblast eGovernmentu nezávisle na úpravě v jiných zákonech. Zvláště pro širokou laickou veřejnost, jíž by měl eGovernment sloužit nejvíce, je velice obtížné se orientovat v tom, co vlastně nabízí a jaké z něj plynou výhody.

2. Základní prvky eGovernmentu v České republice

V České republice je eGovernment popisován prostřednictvím symbolu s názvem eGon, který je obrazně charakterizován jako živý organismus a jednotlivé části e-Governmentu tvoří jeho orgány.

Obrázek č. 2: Postavička eGona, jako symbolu eGovernmentu



Pramen: Ministerstvo vnitra. Dostupné z < http://www.mvcr.cz/clanek/egon-jako-symbol-egovernmentu-moderniho-pratelskeho-a-efektivniho-uradu-252052.aspx >

Mozek celého eGovernmentu je tvořen základními registry veřejné správy. Srdce představuje zákon o datových schránkách. KIVS, tedy Komunikační infrastruktura veřejné správy, která zajišťuje bezpečný přenos dat, tvoří oběhovou soustavu. A nakonec Czech POINT, jakožto soustava kontaktních míst veřejné správy, tvoří prsty eGona.

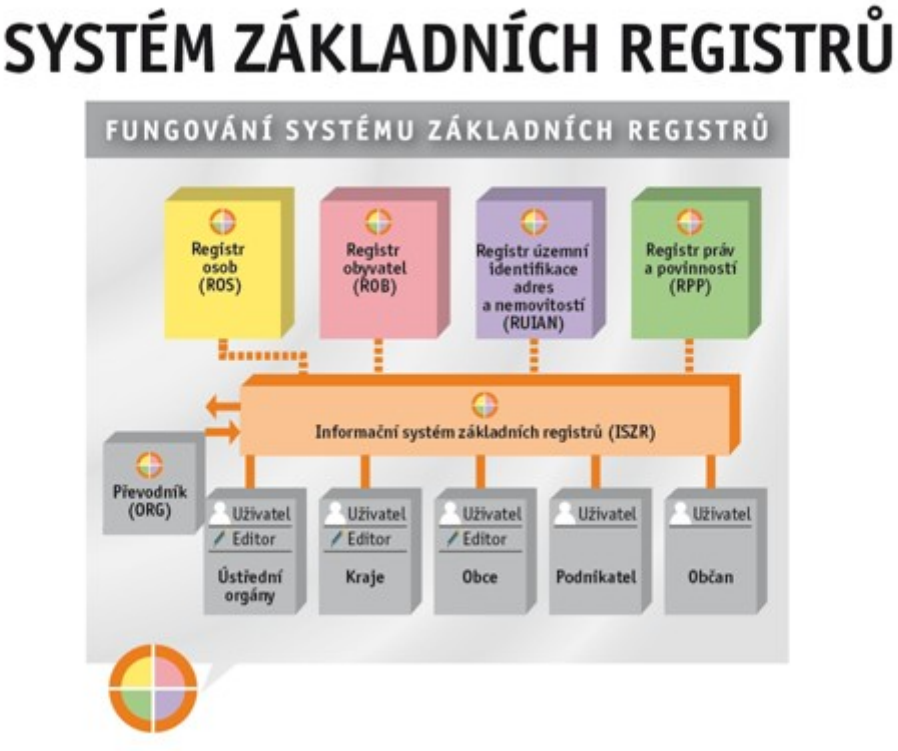
2.1 Základní registry

Snaha o sdílení dat ve veřejné správě a o vytvoření jednotné státní informační soustavy se datuje již do roku 1990 v souvislosti se zahájením činnosti již zmíněné Komise vlády pro

státní informační systémy. Tyto snahy se později promítaly do všech již zmíněných koncepčních a strategických dokumentů vytvořených ať již Úřadem pro státní informační systém či Ministerstvy informatiky nebo vnitra. Postupně docházelo k upřesňování požadavků a představ o funkčnosti základních registrů. Legislativně byly základní registry veřejné správy zakotveny až zákonem o ZR účinným od 1. 7. 2012.

Ustanovením § 3 zákona o ZR byly založeny čtyři registry, označované jako základní. Jsou to registr osob, registr obyvatel, registr územní identifikace a registr práv a povinností. Tyto registry poskytují údaje ústředním orgánům státní správy, krajům, obcím a právnickým osobám a občanům prostřednictvím ISZR, jehož účelem *„je zajišťování sdílení dat mezi jednotlivými základními registry navzájem, základními registry a agendovými informačními systémy a agendovými informačními systémy navzájem, správa oprávnění přístupu k datům a další činnosti podle tohoto zákona.“*[17]

Obrázek č. 3: Systém základních registrů



Pramen: Správa základních registrů. Dostupné z < http://www.mvcr.cz/clanek/zakladni-registry-zakladni-registry-verejne-spravy.aspx>

[17] § 2 písm. f) zákona č. 111/2009 Sb., o základních registrech

Zákon o základních registrech dále vymezuje pojem referenční údaj, a to jako „*údaj, který je v zákoně uvedený jako referenční*“[18]. Referenční údaje jsou následně pro jednotlivé základní registry specifikovány v ust. § 18 odst. 2 zákona o ZR pro registr obyvatel a v ust. § 26 odst. 2 zákona o ZR pro registr osob. Dále zákon o ZR vymezuje pojem agendový informační systém jako „*informační systém veřejné správy, který slouží k výkonu agendy*“[19]. Prostřednictvím agendových informačních systémů se do jednotlivých základních registrů zapisují referenční údaje. Např. do registru osob se zapisují referenční údaje z agendového informačního systému evidence obyvatel, z cizineckého informačního systému, z informačního systému občanských průkazů, informačního systému cestovních dokladů a informačního systému datových schránek. Do registru osob se zapisují údaje z mnohem většího počtu agendových informačních systémů. Mezi nejdůležitější patří veřejné rejstříky právnických a fyzických osob vedené rejstříkovými soudy, dále živnostenský rejstřík, seznam insolvenčních správců, atd. Rovněž je důležitý pojem agenda, jakožto „*souhrn činností spočívajících ve výkonu vymezeného okruhu vzájemně souvisejících činností v rámci působnosti orgánu veřejné moci*“[20]. Posledním pojmem je editor, jenž je zákonem vymezen jako „*orgán veřejné moci, který je oprávněn zapisovat referenční údaje do základního registru a provádět změny zapsaných referenčních údajů.*“[21]

Dle důvodové zprávy k zákonu o ZR je důvodem vzniku základních registrů rozdrobenost právní úpravy informačních systémů veřejné správy, což „*neumožňuje přímo ze zákona komunikaci mezi orgány veřejné moci (a jimi vedenými informačními systémy) vůbec, nebo umožňuje sdílení dat pouze v přesně stanoveném, omezeném rozsahu. Z tohoto důvodu probíhá sdílení dat mezi různými systémy za různých podmínek, a to zejména co do technického provedení. Pro každou vazbu mezi informačními systémy je nutno řešit nové provedení této vazby, přičemž vazby jednoho systému na různé další systémy se mohou uskutečňovat několika různými a vzájemně nekompatibilními způsoby. Tím se zhoršuje interoperabilita informačních systémů, což ve svém důsledku brání dalšímu propojování informačních systémů, a tím výraznějšímu rozšíření moderního výkonu veřejné správy.*“[22]

[18] § 2 písm. b) zákona č. 111/2009 Sb., o základních registrech
[19] § 2 písm. e) zákona č. 111/2009 Sb., o základních registrech
[20] § 2 písm. d) zákona č. 111/2009 Sb., o základních registrech
[21] § 2 písm. g) zákona č. 111/2009 Sb., o základních registrech
[22] Důvodová zpráva k zákonu č. 111/2009 Sb., o základních registrech

Hlavním cílem zákona o ZR, a základních registrů vůbec, je tedy stanovit povinnost orgánům veřejné moci závazně využívat referenčních údajů. S tím je spojena menší administrativní zátěž pro občany a podnikatele, kteří tak nemusí předkládat jednotlivým orgánům veřejné správy stále stejné údaje. To by mělo mít mimo jiné za následek nižší náklady a zvýšení efektivnosti veřejné správy.[23]

Orgánům veřejné správy je však zároveň zaručeno, že referenční údaje mají relevantní právní význam a mohou se na jejich kvalitu spoléhat. Editor je zodpovědný za to, že jím zapsané referenční údaje jsou v souladu s údaji uvedenými v dokumentech, na jejichž základě jsou do příslušného základního registru zapsány. Rovněž byla zavedena presumpce správnosti referenčních údajů, neboť v souladu s ust. § 4 odst. 4 zákona o ZR je *„referenční údaj považován za správný, pokud není prokázán opak nebo pokud nevznikne oprávněná pochybnost o správnosti referenčního údaje.“* Pro případ rozporu referenčních údajů se skutečností je zavedena povinnost orgánů veřejné moci uvědomit o tom neprodleně editora daného referenčního údaje.

Další přidanou hodnotou je snížení technicky a finančně náročného vzájemného propojování možná až tisíců různých více či méně kompatibilních ISVS, které jsou často vytvářeny a spravovány různými externími dodavateli.

2.2 Czech POINT

Zkratka Czech POINT znamená Český Podací Ověřovací a Informační Národní Terminál. Pilotní fáze provozu byla zahájena v roce 2007 a ostrá verze v roce 2008. Jednotlivé funkce Czech POINT se rozšiřují postupně. Hlavním cílem je prostřednictvím dostupné síť poboček Czech POINT zrychlit a zpřístupnit služby orgánů veřejné moci občanům. Smyslem je umožnit občanům, aby na jednom místě získali nejen výpisy z různých evidencí a rejstříků, které vydávají orgány veřejné moci, ale mohli na těchto místech i činit některé úkony vůči orgánům veřejné moci. Činnost Czech POINT tak lze rozdělit do následujících oblastí:

[23] Více např. v dokumentu Přínosy a dopady registru osob ROS, dostupné z http://www.szrcr.cz/uploads/Dokumenty/iop_ROS_letak_prinosy.pdf

1. Vydávání ověřených výstupů z informačních systémů Jedná se např. o výpisy z veřejných rejstříků právnických a fyzických osob, z registru živnostenského podnikání, výpis z katastru nemovitostí, z insolvenčního rejstříku, výpis bodového hodnocení řidiče, atd.
2. Další velkou oblastí činnosti jsou úkony spojené s datovými schránkami, tj. podávání žádostí týkajících se datových schránek a zejména povinnosti vyplývající z autorizované konverze dokumentů (především její provádění).
3. Czech POINT rovněž zprostředkovává příjem některých typů podání občanů vůči orgánům veřejné moci. Jde např. o podání podle živnostenského zákona či podání do registru účastníků provozu modulu autovraků.
4. Dále je možné prostřednictvím Czech POINT interně komunikovat mezi orgány veřejné moci prostřednictvím služby Czech-POINT@office.

Rozsah sítě poboček kontaktních míst je dán vyhláškou č. 364/2009 Sb., o seznamu obecních úřadů a zastupitelských úřadů, které jsou kontaktními místy veřejné správy (vyhláška o kontaktních místech veřejné správy). Kontaktními místy jsou dále některá pracoviště České pošty, s. p. (cca 980 pošt). V současnosti tak existuje více než 7.100 kontaktních míst veřejné správy.

2.3 Datové zprávy a dokumenty v elektronické podobě

Pojem datová zpráva byl do českého právního řádu plnohodnotně zaveden až s nabytím účinnosti zákona o elektronickém podpisu. Datovou zprávou se podle ust. § 2 písm. d) zákona o elektronickém podpisu rozumí „*elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na technických nosičích dat, používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložená na technických nosičích ve formě datového souboru*.“ V době nabytí účinností zákona o elektronickém podpisu byly nejčastějším typem datové zprávy zasílané na elektronické adresy (e-mail). S nabytím účinnosti zákona o DS došlo k podstatnému rozšíření tohoto pojmu, kdy ust. § 19 odst. 1 zákona o DS stanoví, že „*dokumenty orgánů veřejné moci doručované prostřednictvím datové schránky, úkony prováděné vůči orgánům veřejné moci prostřednictvím datové schránky a dokumenty fyzických osob, podnikajících fyzických osob a právnických osob dodávané prostřednictvím datové schránky mají formu datové zprávy.“* Vyhláška č. 259/2012 Sb., pak

označuje za datové zprávy i ty, které jsou přenášeny na technických nosičích dat. Zároveň počítá s tím, že mohou existovat i další typy datových zpráv.

Definice dokumentu je uvedena v ust. § 2 písm. e) zákona o archivnictví, přičemž dokumentem se „*rozumí každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena; za dokument vzniklý z činnosti původce se považuje rovněž dokument, který byl původci doručen nebo jinak předán.“*

Pojmosloví uvedené v jednotlivých zákonech však není jednotné. Např. § 11 odst. 1 zákona o elektronickém podpisu hovoří „*o podepisování nebo označování dokumentu v podobě datové zprávy.“* Stejně tak zmíněný § 19 zákona o DS. Vyhláška č. 259/2012 Sb. pak používá sousloví „*datová zpráva a dokument v ní obsažený.“*[24] Podle některých autorů tvoří u datových schránek „*datovou zprávu obálka a obsah datové zprávy.“*[25] Obsahem datové zprávy může být jedna či více příloh (dokumentů), které jsou pro zasílání datovými schránkami povoleny vyhláškou č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

Je tedy nutno rozlišovat mezi datovou zprávou v širším smyslu, kterou si lze představit jako obálku, která slouží k přenášení elektronických dat a je tak nadřazena pojmu dokument v elektronické podobě. Podle tohoto výkladu se do datové zprávy elektronické dokumenty vkládají a spolu s datovou zprávou přenášejí. V užším slova smyslu, tak, jak je používá zákon o elektronickém podpisu, je pojem datové zprávy identický s pojmem elektronický dokument. Lze je považovat tedy za synonyma. Dle mého názoru je třeba používat pojem datové zprávy v širším smyslu, tedy jako obálku či nosič, sloužící k přenosu elektronických dat z jednoho místa na druhé. K datové zprávě je možné přiložit elektronický dokument a ten spolu s datovou zprávou poslat. Mezi nejčastější datové zprávy v tomto smyslu lze pak považovat e-maily či datové zprávy zasílané datovými schránkami.

S rozvojem informační společnosti a eGovernmentu stoupá i počet, evidencí, seznamů, databází, písemností, dokumentů, atd., jež jsou vedeny výlučně v elektronické podobě

[24] např. § 6 odst. 1 písm. a) vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby
[25] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2. vydání. Leges, 2012. s 163

prostřednictvím výpočetní techniky a informačních systémů. Opouští se představa, že každý dokument musí mít písemný (analogový) originál, z něhož vznikl (např. skenováním). Písemnosti mohou tedy primárně vzniknout v elektronické podobě. S tím souvisí nutnost legislativní úpravy vzniku elektronických dokumentů, způsobů převodu z elektronické do analogové podoby, dále zajištění důvěryhodnosti pravosti elektronických dokumentů, ale i jejich krátkodobá a dlouhodobá archivace. Dalším velkým úkolem je legislativně upravit „rovnoprávnost" mezi analogovými a elektronickými (digitálními) dokumenty. S tím souvisí úprava jejich využití ve správním či soudním řízení při výkonu veřejné moci. Za hlavní krok k praktické použitelnosti elektronických dokumentů lze považovat až přijetí zákona o elektronickém podpisu a přijetí zákona o DS.

„*Elektronický dokument má řadu specifických vlastností. Nejvýraznější je přístup k originalitě či jinými slovy postavení originálu dokumentu. V případě elektronického dokumentu totiž originál v klasickém pojetí ztrácí smysl.*"[26] Důvodem je absence pevného spojení s jednoznačným nosičem, který u listinných dokumentů tvoří jeden konkrétní list papíru.

V obecném povědomí, ale i českém právním řádu se používají pojmy jako písemnost, listina nebo dokument a dochází k jejich vzájemnému zaměňování. Platná legislativa pouze v zákoně o archivnictví vymezuje již zmíněnou definici dokumentu. Zákon tak rozeznává analogové (někdy označované jako listinné) a digitální (elektronické) dokumenty. Nedefinovaným pojmem je písemnost. Písemnosti rovněž rozdělujeme na ty v listinné (analogové) podobě, jenž jsou obsaženy nejčastěji na listech papíru. List papíru je tak nosič. Písemnost v elektronické (digitální) podobě může být obsažena nejčastěji v dokumentu v elektronické podobě nebo v datové zprávě. Datové zprávy a dokumenty jsou tedy rovněž nosiče.

Elektronické dokumenty mohou vznikat dvěma základními způsoby:

1. Pomocí textového editoru či jiného obdobného programu,
2. Jako elektronická kopie dokumentu, který vznikl v listinné podobě (prosté skenování, konverze, autorizovaná konverze či jiný převod z digitální do analogové podoby).

Elektronické dokumenty mohou obsahovat např. smlouvy, faktury, rozličná právní jednání, ale i rozhodnutí správních orgánů či soudů, atd. Z hlediska eGovernentu jsou ve středu zájmu

[26] LECHNER, Tomáš. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013, s. 40

zejména elektronické dokumenty obsahující podání učiněná vůči orgánům veřejné moci a rozhodnutí orgánů veřejné moci v elektronické podobě. Prostřednictvím datových zpráv a dokumentů v nich obsažených lze zasílat orgánům veřejné moci podání v elektronické podobě. Podání tak tvoří samotný text datové zprávy či dokumentu. U některých typů datových zpráv, např. u e-mailu může být podání v elektronické podobě obsaženo přímo v těle datové zprávy, u jiných typů datových zpráv, např. zprávy z datové schránky, může být podání obsaženo pouze v přiloženém dokumentu.

Vyhláška č. 259/2012 Sb., která s účinností od 1. 7. 2012 nahradila vyhlášku č. 496/2004 Sb., o elektronických podatelnách, stanovují povinnost veřejnoprávního původce (ust. § 3 odst. 1 zákona o archivnictví) vybavit podatelnu zařízením umožňujícím příjem datových zpráv doručovaných:

- na elektronické adresy (e-mail),
- na přenosných technických nosičích dat,
- prostřednictvím datové schránky.

Vyhláška č. 259/2012 Sb. stanoví i další povinnosti, ale i oprávnění veřejnoprávních původců, které se týkají příjmu datových zpráv a dokumentů v nich obsažených. Konkrétně se jedná o:

- povinnost zveřejňovat informace o provozu podatelny a o podmínkách přijímání datových zpráv a dokumentů na úřední desce (např. e-mailovou adresu, identifikátor datové schránky, úřední hodiny podatelny, další možnosti elektronické komunikace, které veřejnoprávní původce připouští, přehled přijímaných datových formátů dokumentů atd.,
- možnost v případě doručení poškozeného dokumentu, který nelze zobrazit uživatelsky vnímatelným způsobem nebo obsahuje škodlivý kód, takový dokument nepřijímat. S tím je spojena povinnost o tomto vyrozumět podatele, pokud je známa jeho elektronická adresa nebo jiné kontaktní údaje,
- povinnost u datové zprávy a dokumentu v něm obsaženého zjišťovat, zda jsou splněny podmínky příjmu (např. povolené datové formáty dokumentů), dále zjišťovat, zda jsou datová zpráva a dokument podepsány elektronickým podpisem, označeny elektronickou značkou, zda je připojeno časové razítko a zda jsou podpis a značka založeny na kvalifikovaných, resp. kvalifikovaných systémových certifikátech,
- povinnost sestavit o výsledcích ověřování datové zprávy a dokumentů záznam,

- povinnost vyrozumět podatele o příjmu jeho datové zprávy a o výsledcích jejího ověřování.

Co se týče datových formátů dokumentů, které musí veřejnoprávní původci přijímat, je úprava obsažena v ust. § 64 odst. 1 zákona o archivnictví, který poněkud složitě a nejasně stanoví povinnost přijímat datové formáty stanovené jako výstupní datové formáty (tzn. ty vyjmenované v § 23 vyhlášky č. 259/2012 Sb.) nebo formáty dokumentů, které jsou výstupem z autorizované konverze (zde odkazuje dle mého názoru na vyhlášku č. 193/2009 Sb.).

Podle tohoto výkladu tedy veřejnoprávní původci musí přijímat dokumenty v datových formátech PDF, PNG, TIF, TIFF, JPEG/JFIF, MPEG-2, MPEG-1, GIF, MP2, MP3, WAV, PCM a za určitých podmínek i XML. Naopak nemusí přijímat relativně časté datové formáty DOC, DOCX (Word), XLS, XLSX (Excel) či ZFO. Tato úprava však nekoresponduje s přílohou č. 3 vyhlášky č. 194/2009 Sb., která připouští zasílat datovými schránkami mnohem větší počet datových formátů dokumentů, což může být pro veřejnost matoucí.

2.4 Elektronický podpis, elektronická značka a časové razítko

Jak již bylo uvedeno, s nabytím účinnosti zákona o elektronickém podpis k 1. 10. 2000 byly poprvé legislativně vymezeny podmínky pro možnost podepisování, resp. označování elektronických dokumentů elektronickým podpisem či elektronickou značkou.

Zároveň došlo k novelizaci některých procesních předpisů, jimiž byla stanovena povinnost orgánům veřejné správy přijímat podání podepsaná elektronickým podpisem. Jednalo se o zákon č. 71/1967 Sb., o správním řízení (správní řád), který v § 19 odst. 1 nově stanovil, že „p*odání lze učinit písemně nebo ústně do protokolu nebo v elektronické podobě podepsané elektronicky podle zvláštních předpisů. Lze je též učinit telegraficky; takové podání obsahující návrh ve věci je třeba písemně nebo ústně do protokolu doplnit nejpozději do 3 dnů.“* Dále o.s.ř., podle jehož ust. § 42 odst. 1 bylo možno „*podání učinit písemně, ústně do protokolu, v elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky nebo telefaxem.“* Obdobnou úpravu obsahoval nově i trestní řád. Došlo tak ke zrovnoprávnění listinných a elektronických podání, která jsou podepsána elektronickým podpisem.

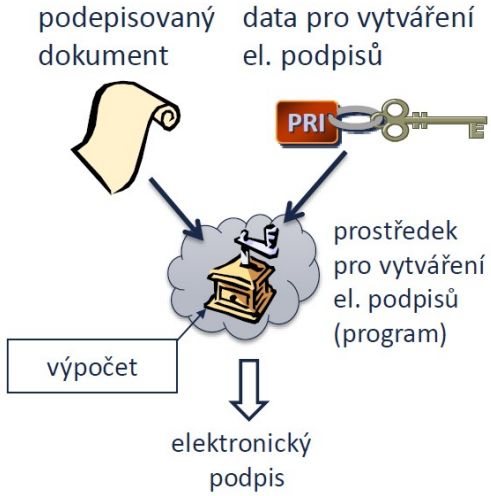
Došlo i k úpravě hmotného práva, konkrétně zákona č. 40/1964 Sb., občanský zákoník, podle jehož ust. § 40 odst. 3 *„je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.“*

2.4.1 Elektronický podpis

Z hlediska práva lze podpis popsat jako právní institut, kterým určitá osoba projevila svůj souhlas s obsahem popřípadě s platností určitého dokumentu. Aby mohlo dojít k plnohodnotnému využívání elektronických dokumentů, musí zde existovat rovněž plnohodnotná alternativa vlastnoručního podpisu. Zákon o elektronickém podpisu definuje elektronický podpis jako *„údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.“*[27] Z tohoto vyplývají dvě základní kritéria, která musí elektronický podpis splňovat. 1. Elektronický podpis je vždy spjat s datovou zprávou (dokumentem) a nemůže tak existovat sám o sobě. 2. Musí být možné zjistit identitu osoby, která datovou zprávu (dokument podepsala).

Vytváření elektronického podpisu lze znázornit následovně:

Obrázek č. 4: Tvorba elektronického podpisu



Pramen: Jiří Peterka, Jan Podaný, Podstata a vlastnosti elektronických podpisů, dostupné z < http://asja.jacz.cz/index.php?pageid=1002&task=7&course_id=2477>

[27] § 2 písm. a) zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

Zákon o elektronickém podpisu v současné době definuje v podstatě 3 stupně elektronických podpisů:

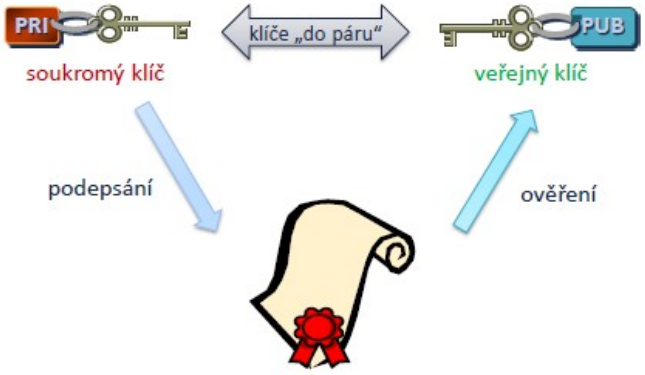
Tabulka č. 1: Typy elektronických podpisů

El. podpis	Definice elektronického podpisu	Certifikát, na kterém je podpis založen
Obyčejný - § 2 písm. a)	Údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě	Obyčejný - § 2 pism. k) Není zde žádná záruka ověření podatele – podatel si certifikát může vytvořit sám.
Zaručený - § 2 písm. b)	Zaručeným podpisem se rozumí elektronický podpis, který splňuje následující požadavky: 1. je jednoznačně spojen s podepisující osobou, 2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, 3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, 4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,	Kvalifikovaný - § 2 písm. l) + § 12 Certifikát může být vydán i neakreditovaným poskytovatelem certifikačních služeb (prakticky kdokoliv)
Uznávaný - § 2 písm. b) + § 11	Uznávaným elektronickým podpisem se rozumí: a) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby, b) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie	Kvalifikovaný - § 2 písm. l) + § 12 Certifikát musí být vydaný akreditovaným poskytovatelem certifikačních služeb

Pramen: Vytvořeno autorem

Abychom mohli zjistit totožnost osoby, která datovou zprávu či dokument podepsala, musí existovat subjekt, který poskytne informace, komu elektronický podpis patří. Jde tedy o spárování informací o držiteli certifikátu (soukromého klíče) a veřejně dostupných informací o jeho držiteli (veřejný klíč).

Obrázek č. 5: Ověřování elektronických podpisů



Pramen: Jiří Peterka, Jan Podaný, Podstata a vlastnosti elektronických podpisů, dostupné z < http://asja.jacz.cz/index.php?pageid=1002&task=7&course_id=2477>

Po technické stránce lze zaručený a uznávaný podpis považovat za totožné. Rozdíl je zde v institucionálním zajištění vydavatele certifikátu a tím i vyšší důvěryhodnosti při identifikaci podepisující osoby. Zatímco u zaručeného podpisu může certifikát (soukromý klíč) vydat kdokoliv, u uznávaného certifikátu to mohou být pouze akreditovaní poskytovatelé certifikačních služeb (rovněž označovaní jako certifikační autority), což jsou osoby, kterým byla udělena Ministerstvem vnitra ČR akreditace a nad nimiž je vykonáván podrobný dohled v souladu se zákonem o elektronickém podpisu.

Podání učiněná vůči orgánům veřejné moci musí být podepsána uznávaným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaným akreditovaným poskytovatelem certifikačních služeb tak, jak je jej upravuje ust. § 11 zákona o elektronickém podpisu. Jde tedy o podpis v nejvyšší kvalitě založený na certifikátu, z něhož lze jednoznačně identifikovat podpisující osobu. V praxi se při vydávání kvalifikovaného certifikátu vyžadují dva průkazy totožnosti osoby, která o něj žádá.

V současné době působí na území České republiky 3 certifikační autority, a to:

- První certifikační autorita a.s., IČ 264393 95, www.ica.cz,
- Česká pošta, s. p., IČ 47114983, www.postsignum.cz,
- eIdentity a. s., IČ 27112489, www.eidentity.cz.

Pokud by podání vůči orgánu veřejné moci bylo podepsáno běžným podpisem či pouze zaručeným elektronickým podpisem, bylo by na takové podání nahlíženo jako na nepodepsané.

V souladu se směrnicí Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy v některém ze členských států EU a Rozhodnutí komise 2009/767/ES, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“, podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu a v souladu s ust. § 9 odst. 2 písm. g) zákona o elektronickém podpisu Ministerstvo vnitra ČR vede a zveřejňuje způsobem umožňujícím dálkový přístup seznam důvěryhodných certifikačních služeb poskytovatelů, kteří působí na území Evropské unie. Rovněž tyto certifikáty musí členské státy v souladu se směrnicí uznávat jako kvalifikované. Seznam důvěryhodných certifikátů je veden v aplikaci CertlQ zveřejněné na stránkách http://tsl.gov.cz/.

Platnost kvalifikovaných certifikátů vydaných v České republice je 1 rok, a to z důvodu garance zabezpečení, že po tuto dobu nedojde k jejich technickému prolomení. V jiných státech EU je však platnost certifikátu delší. Je tedy otázkou, do jaké míry jde o vliv poskytovatelů na znění zákona o elektronickém podpisu. Před uplynutím této doby může být certifikát zneplatněn. Důvodem může být ztráta soukromého klíče či jeho kompromitace, dále úmrtí osoby, které byl certifikát vydán, technické problémy s certifikátem a u zaměstnanců, kteří jej využívají při své pracovní činnosti, skončení pracovního poměru, atd. Zneplatnění certifikátu musí certifikační autorita uvádět v seznamu zneplatněných certifikátů (tzv. CRL seznamy), které musí zveřejňovat minimálně jednou za 24 hodin.

2.4.2 Elektronická značka

Právní úprava elektronické značky byla do zákona o elektronickém podpisu vložena zákonem č. 440/2004 Sb. s účinností od července 2004. Hlavním smyslem jejího používání je umožnit zvýšení důvěryhodnosti dokumentů, aniž by musel být každý z nich podepisován

elektronickým podpisem. Stejně jako u elektronického podpisu, tak i u elektronické značky rozlišuje zákon o elektronickém podpisu 3 typy značek a stejně tak stanoví, že vůči orgánům veřejné moci lze podání označovat pouze uznávanou elektronickou značkou. Po technické stránce jsou elektronické značky téměř naprosto identické jako elektronické podpisy, rozdíly jsou zejména legislativního charakteru.

Rozdíly mezi elektronickou značkou a elektronickým podpisem jsou:

- u elektronického podpisu podepisující osoba svým podpisem stvrzuje, že obsah datové zprávy či dokumentu byl zkontrolován po obsahové stránce; u elektronické značky však nelze jednoznačně vyvodit, že dokument, který byl označen, skutečně označující osoba zkontrolovala či jej vůbec četla,
- elektronickou značkou se tedy zaručuje pouze, že nedošlo od označení datové zprávy či dokumentu k její změně,
- datové zprávy a dokumenty mohou být (a většinou jsou) označovány elektronickou značkou automaticky, např. počítačem či serverem,
- v kvalifikovaném certifikátu, na jehož základě se tvoří elektronická značka, může být uvedena jako držitel certifikátu i právnická osoba (obchodní společnost, orgán veřejné moci, orgán územní samosprávy, atd.),
- v pojmosloví; elektronické podpisy jsou založeny na certifikátu, zatímco značky na systémovém certifikátu; datové zprávy a dokumenty se elektronickým podpisem podepisují, zatímco značkami označují,
- na rozdíl od elektronického podpisu neupravují procesní předpisy (správní řád, o.s.ř., atd.) výslovně možnost podání označeného uznávanou elektronickou značkou.

2.4.3 Časové razítko

Zákonem č. 440/2004 Sb. byl rovněž zaveden pojem kvalifikované časové razítko. Podle ust. § 2 písm. r) zákona o elektronickém podpisu se „*kvalifikovaným časovým razítkem rozumí datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem*.“

Hlavním účelem časového razítka je zafixovat dokument v čase. Připojuje se k dokumentům jako důkaz, že v daném čase a v dané podobě existovaly. Časové razítko obsahuje datum a čas vydání, číslo časového razítka a identifikaci třetí strany, která časové razítko vydala (poskytovatele certifikačních služeb). Opět jej mohou vydávat pouze akreditovaní poskytovatelé certifikačních služeb. Tento čas připojuje k dokumentu certifikační autorita, proto údaji o čase lze důvěřovat. Pokud byl dokument elektronicky podepsán či označen před přidáním časového razítka, tak přidáním časového razítka se prodlužuje platnost elektronického podpisu či značky (nikoliv certifikátu), a to po dobu platnosti kvalifikovaného časového razítka. Razítka mohou být přikládána i opakovaně a postupně. Proto mohou platnost podpisu z původního jednoho roku prodloužit na desítky let.

2.4.4 Ověřování elektronických podpisů a značek

Postup při ověřování elektronických podpisů je stanoven vyhláškou č. 212/2012 Sb., o ověřování platnosti zaručeného elektronického podpisu. Vyhláška stanoví jak technické, tak metodické náležitosti postupu ověřování. Stanoví dva okamžiky, ke kterým se ověřuje platnost elektronického podpisu a značky a nově zohledňuje při okamžiku ověřování i přidání časového razítka. Dále vyhláška určuje, že při ověřování je nutné provádět kontrolu oproti seznamu zneplatněných certifikátů (tzv. CRL seznamy).

Co však vyhláška naprosto postrádá, je postup při ověřování a vyhodnocování vícenásobných podpisů datové zprávy a dokumentu. Vyhláška také nezohledňuje *„rozhodnutí Evropské komise č. 2011/130/ES, které uložilo členským zemím používat nové formáty elektronických podpisů (tzv. referenční formáty).“*[28]

2.5 Datové schránky a autorizovaná konverze dokumentů

Jednou z hlavních náplní e-Governmentu je umožnit snadnou a dostupnou elektronickou komunikaci občanů s orgány veřejné moci. S tím je však spojena i nutnost zajištění věrohodnosti a autentičnosti zasílaných elektronických dokumentů a možnost ověřit identitu odesílající osoby, ale i adresáta. Běžně dostupná komunikace, jako např. e-mail, však

[28] Peterka, J. Jak budou fungovat elektronické podpisy po 1. červenci? [online]. Vydáno 26. 5. 2012 [cit. 3. 2. 2014]. Dostupné z: < http://www.lupa.cz/clanky/jak-budou-fungovat-elektronicke-podpisy-po-1-cervenci/>

z hlediska spolehlivosti a bezpečnosti nemůže veškeré požadavky naplnit. Proto jsou ve vyspělých zemích zaváděny instituty eGovernentu, které mají právě takovou snadnou a bezpečnou komunikaci zajistit. V České republice jsou to datové schránky a autorizovaná konverze dokumentů, které byly do českého právního řádu zavedeny již zmíněným zákonem o DS.

Jde o institut eGovernmentu, který je v Evropě, ale i ve světě unikátní zejména v tom, že v České republice jsou datové schránky pro některé subjekty zřízeny povinně ze zákona. Stejně tak zákon o DS pro některé subjekty stanovil povinnost komunikovat mezi sebou pouze prostřednictvím jejich datových schránek.

Za hlavní důvody vzniku datových schránek a autorizované konverze se uvádí nedostatečná dřívější úprava elektronické komunikace s orgány veřejné moci zavedená zákonem o elektronickém podpisu. „*Díky resortní roztříštěnosti a odlišným zájmům, ale i mnoha jiným, často spíše psychologickým faktorům, byla problematika podávání a doručování elektronickou, ale i „klasickou" cestou u nás upravena všelijak, jen ne jednotně a srozumitelně.*"[29] Za další velký problém lze označit dřívější úpravu doručování účastníkům správního a soudního řízení, zejména těm, kteří se doručení správního či soudního rozhodnutí záměrně a cíleně vyhýbali. To se týkalo fyzických, ale i právnických osob, kterým bylo téměř nemožné doručovat na adresu neexistujícího sídla.

2.5.1 Datové schránky

Podle důvodové zprávy k zákonu o DS hlavním cílem „*zavedení institutu datových schránek pro doručování je přiblížení orgánu veřejné moci občanovi prostřednictvím elektronických nástrojů, zefektivnění komunikace mezi občanem a orgánem veřejné moci a komunikace mezi orgány veřejné moci.*"[30]

Sám zákon o DS definuje datovou schránkou jako „*elektronické úložiště, které je určeno k*
a) doručování orgány veřejné moci,
b) provádění úkonů vůči orgánům veřejné moci,

[29] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2. vydání. Leges, 2012. s 163
[30] Důvodová zpráva k zákonu č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

c) dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.“[31]

Osobně se mi zdá tato definice ne úplně přesně popisující skutečný účel a funkci datových schránek. Ze zákonné definice by se mohlo zdát, že hlavním smyslem datových schránek je dlouhodobě ukládat elektronická data, resp. datové zprávy, což není pravda. Datové zprávy se v souladu s ust. § 6 vyhlášky č. 194/2009 Sb. ukládají v informačním systému datových schránek (dále jen „ISDS“) přesně po dobu 90 dnů ode dne dodání. Vlastník datové schránky si tedy takové zprávy nemůže z vlastní datové schránky dříve odstranit. Pro trvalejší archivaci datových zpráv je třeba využít placenou službu označovanou jako Datový trezor.

Hlavním účelem datových schránek je umožnit bezpečnou a spolehlivou komunikaci mezi orgány veřejné moci a občany a právnickými osobami. Lepší definici pak lze nalézt přímo na internetových stránkách www.datoveschranky.info, podle které datové schránky slouží „*pro komunikaci v oblasti veřejné správy. Jejím prostřednictvím lze činit podání kterémukoliv úřadu. Úřady prostřednictvím datové schránky doručují své písemnosti příslušným adresátům (fyzickým nebo právnickým osobám), stejně jako komunikují s jinými orgány veřejné správy. Veškerým úkonům, které jsou prostřednictvím elektronické datové schránky, resp. přepážky činěny, je přiznána ekvivalence k úkonům činěným písemně.“*[32]

Ale ani tato definice není úplně přesná, protože nezohledňuje zákon č. 190/2009 Sb., kterým došlo k novelizaci zákona o DS. Touto novelou bylo umožněno, aby soukromé subjekty (fyzické, podnikající fyzické a právnické osoby) komunikovaly prostřednictvím datových schránek mezi sebou. Datová schránka tedy od této novely „*funguje jako něco, co bychom mohli nazvat e-mail2 – tedy zákon poskytuje možnost používání datových schránek jako důvěryhodného (autentizovaného) a zabezpečeného e-mailu mezi soukromými subjekty navzájem.“*[33]

Po technické stránce jde o technologii zabezpečenou, využívající šifrované spojení mezi uživateli a ISDS. ISDS je podle ust. § 14 odst. 1 výslovně označen za ISVS v souladu se zákonem o ISVS a jeho správcem je Ministerstvo vnitra ČR. Obsahuje informace o datových

[31] § 2 odst. 1 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

[32] *Webový portál datových schránek* [online] [cit. 19. 3. 2014]. Dostupné z: < http://www.datoveschranky.info/cz/o-datovych-schrankach/slovnik-pojmu-id34696/>.

[33] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2. vydání. Leges, 2012. s 169

zprávách a jejich uživatelích. Seznam držitelů datových schránek je dle ust. § 14b zákona o DS součástí ISDS a je veřejně přístupný (přes internetové stránky www.datoveschranky.info). Tento seznam se člení na samostatné části pro fyzické osoby, podnikající fyzické osoby, pro právnické osoby a pro orgány veřejné moci. Náležitosti seznamu jsou uvedeny v zákoně o DS. V zákoně je přímo uvedena povinnost využívat za účelem správy ISDS referenční údaje ze základních registrů. Jak již bylo uvedeno, podle ust. § 19 zákona o DS dokumenty doručované prostřednictvím datové schránky mají formu datové zprávy. Povolené datové formáty dokumentů, které mohou být datovou schránkou zaslány, jsou v příloze č. 3 vyhlášky č. 194/2009 Sb.

Komunikaci prostřednictví datových schránek lze členit na:

1. povinnou ze zákona

- komunikace mezi orgány veřejné moci vzájemně (ust. § 17 zákona o DS),
- komunikace orgánů veřejné moci vůči právnickým, podnikajícím fyzickým a fyzickým osobám, kterým byla datová schránka zřízena ze zákona nebo na jejich žádost (ust. § 17 zákona o DS).

2. nepovinnou

- komunikace fyzických, podnikajících fyzických a právnických osob vůči orgánům veřejné moci (ust. § 18 zákona o DS),
- komunikace mezi fyzickými, podnikajícími fyzickými a právnickými osobami navzájem (ust. § 18a zákona o DS).

Výjimky jsou stanoveny rovněž zákonem o DS.

Datové schránky se zřizují buď ze zákona, nebo na žádost. Povinně musí mít zřízenu datovou schránku orgány veřejné moci, právnické osoby zřízené zákonem, právnické osoby zapsané v obchodním rejstříku, insolvenční správci, advokáti a daňoví poradci. Pro posledně jmenované advokáty a daňové poradce byla v zákoně stanovena výjimka z povinnosti mít zřízenu datovou schránku, která však skončila 1. července 2012. Na žádost může být zřízena kterékoliv jiné právnické osobě (která není zapsána v obchodním rejstříku), podnikající fyzické osobě či fyzické osobě. Zřízení datové schránky je bezplatné a žádosti musí být vyhověno do 3 dnů ode dne podání žádosti.

2.5.2 Autorizovaná konverze

Nutnou podmínkou zavedení široké elektronické komunikace je jednoznačné legislativní zakotvení zrovnoprávnění listinných a elektronických dokumentů a podání. Autorizovaná konverze je upravena v ust. § 22 a následujících zákona o DS a rozumí se jí:

a) „*úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky, nebo*
b) *úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky*."

„*Jedná se o kvalifikovanou formu převodu spočívající ve změně formy dokumentu, při které je zachována autentičnost dokumentu a integrita vazby mezi převáděným a výsledným dokumentem.*"[34] Jinak řečeno dokument, který autorizovanou konverzí vznikl, má stejné právní účinky a právní sílu jako dokument, z něhož vznikl.

Konverzi provádí z moci úřední orgán veřejné moci. Na žádost ji pak provádí Czech POINT a advokáti (dle zákona o advokacii).

2.6 Spisové služby v elektronické podobě

Vedení spisové služby v elektronické podobě lze považovat za jednu z nejdůležitějších částí eGovernentu. Jde o část označovanou jako eSpráva, tedy služby G2G. Od vedení spisové služby v elektronické podobě je třeba rozlišovat vedení spisů v elektronické podobě, které povinné není. Velice jednoduše řečeno, spisová služba obecně slouží k evidenci spisů označených spisovými značkami a dále k evidenci jednotlivých dokumentů ve smyslu spisového přehledu (nikoliv samotných elektronických dokumentů). Ve spisové službě se zejména sleduje vytváření spisů, spisový oběh a jejich vyřizování. Dále spisové služby často

[34] BUDIŠ, Petr a Iva HŘEBÍKOVÁ. *Datové schránky: fungování, doručování, bezpečnost, návody*. 1. vyd. Olomouc: ANAG, 2010, s. 209

umožňují odesílat jejich prostřednictvím dokumenty do datové schránky a plní řadu jiných funkcí dle specifické náplně činností konkrétního orgánu veřejné moci.

2.7 Další prvky e-Governmentu v České republice

Datové schránky, základní registry a Czech POINT jsou nejdůležitějšími nástroji e-Governmentu v České republice, ale nejsou zdaleka jedinými. S ohledem na cíl této práce zmíním dané nástroje pouze okrajově. Ministerstvo vnitra ČR zařazuje mezi prvky eGovernmetu dále portál veřejné správy, elektronický občanský průkaz nebo centrální místo služeb. Lze sem zajisté zařadit i elektronickou sbírku zákonů a sbírku mezinárodních smluv, které byly spuštěny k 1. 12. 2010. V roce 2011 byl zahájen projekt Národního digitálního archivu, jehož účelem je dlouhodobá archivace elektronickým dokumentů. Původní termín dokončení realizace v roce 2013 byl posunut na 30. 6. 2015.

Poněkud stranou dosavadního vývoje stojí tzv. e-demokracie, a to ať již jde o možnost volit zástupce elektronickým hlasováním, tak se prostřednictvím tzv. e-participace podílet na posílení demokratizace veřejné správy. Přestože se o možnostech elektronického hlasování ve volbách do Parlamentu i zastupitelstev územních samosprávných celků uvažuje delší dobu, a to i ohledem na stále klesající účast občanů ve volbách, žádné konkrétní kroky k zavedení elektronického hlasování učiněny nebyly. MK prvkům e-participace lze zařadit i různá, elektronickými způsoby realizovaná, diskusní a připomínková řízení. V České republice je možné již delší dobu sledovat on-line jednání Poslanecké sněmovny i Senátu a na internetových stránkách obou komor jsou pravidelně zveřejňovány návrhy zákonů včetně důvodových zpráv, stejně tak zápisy z jednání a výsledky hlasování. U krajů již on-line zveřejňování jednání zastupitelstev pravidlem není, stejně tak u obcí. Již v roce 2008 byla usnesením vlády č. 879 ze dne 13. 8. 2007 schválena metodika pro zapojování veřejnosti do přípravy vládních dokumentů.[35]

Značně diskutovanou problematikou jsou tzv. otevřená data, která se rovněž dají zařadit mezi prvky e-participace, pro kterou je jednou z hlavních podmínek informovanost o činnosti

[35] Více např. v dokumentu Zpráva o vyhodnocení pilotních projektů pro ověření funkčnosti metodiky pro zapojování veřejnosti do přípravy vládních dokumentů, dostupné z http://www.mvcr.cz/soubor/zprava-o-vyhodnoceni-pilotnich-projektu-pro-overeni-funkcnosti-metodiky-pro-zapojovani-verejnosti.aspx.

orgánů veřejné moci. Otevřená data „*jsou informace a čísla bezplatně a volně dostupná na internetu ve strukturované a strojově čitelné podobě a jsou zpřístupněna způsobem, který jejich využití neklade zbytečné technické či jiné překážky*.“[36] Zveřejňovanými údaji mohou být informace o činnosti orgánů veřejné moci, zápisy z jednání organizací, informace o jejich rozpočtu, nakládání s finančními prostředky, informace z oblasti životního prostředí, z oblasti sociálních služeb, dále např. hodnocení nemocniční péče a mnoho dalších. Nevládní neziskové organizace vyvíjí neustálý tlak na zveřejňování dat ze strany orgánů veřejné moci, a to i nad rámec zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Jsou pořádány různé soutěže o nejlepší a naopak nejhorší přístup orgánů veřejné moci ke zveřejňování dat. Jako příklad lze uvést soutěž o nejlepší webové stránky obcí Zlatý erb či soutěže pořádané Fondem Otakara Motejla. Problematika otevřených dat je jedním z úkolů Strategie vlády v boji s korupcí na období 2013 a 2014 schválené usnesením vlády č. 39 ze dne 16. 1. 2013 a je rovněž zohledněna v Akčním plánu s názvem Partnerství pro otevřené vládnutí, který byl připraven na základě usnesení vlády č. 691 ze dne 14. 9. 2014.

2.8 Shrnutí kapitoly

Zavedením elektronických podpisů, datových schránek a základních registrů byl dle mého názoru postaven základ k dalšímu rozvoji eGovernmentu, zejména co se týče komunikace s orgány veřejné moci a sdílení údajů mezi orgány veřejné moci. Prvky e-participace, i přes početná vládní usnesení, analýzy, akční plány a hodnotící zprávy, nebyly dosud do právního řádu a praxe orgánů veřejné moci plně zavedena. Nicméně je zde neustále ze strany veřejnosti vyvíjen tlak a domnívám se, že v této oblasti dojde k rychlému vývoji.

[36] *Webový portál OtevřenáData.cz* [online] [cit. 15. 10. 2014]. Dostupné z: < http://www.otevrenadata.cz/ otevrena-data /co-jsou-otevrena-data/>.

3. eJustice jako součást eGovernmentu

I v oblasti justice (soudy, státní zastupitelství, probační a mediační služba, vězeňská služba a Justiční akademie), kde je ústředním orgánem státní správy Ministerstvo spravedlnosti, byly v posledních letech učiněny výrazné kroky při zavádění elektronických nástrojů e-Governmentu. Z povahy jednotlivých orgánů justice vyplývá, že největší oblast možností zavádění e-Governmentu je u soudů, ale elektronizace se dotýká i ostatních orgánů justice. Pro elektronizaci justice se vžilo označení eJustice, kterou tak můžeme považovat za součást e-Governmentu.

Stejně jako e-Government, tak i výraz eJustice není v žádném právním předpise definován. Ani samo Ministerstvo spravedlnosti nenabízí definici. V literatuře lze nalézt definici, podle které eJustice *„znamená využití informačních technologií a systémů v prostředí justice (resortu spravedlnosti), především pak zavedení elektronické formy komunikace, výměny a zpracování informací mezi subjekty, nacházejícími se v prostředí justice nebo vstupujícími do kontaktů s resortem justice (účastníci řízení, jiné orgány veřejné moci).“*[37]

Dle mého názoru by se eJustice dala stručně definovat jako využití informačních a komunikačních technologií v justici s cílem zajistit efektivní fungování a rychlé rozhodování organizací justice.

Rozšířenou definici eJustice bych pojal jako využití informačních a komunikačních technologií v justici s cílem zajistit efektivní vedení spisové služby, získávání informací důležitých pro rozhodování a umožnit snadnou a uživatelsky přívětivou vzájemnou elektronickou komunikaci účastníků a organizací justice.

Ani jedna z definic však nedokáže popsat složitost a vzájemnou propojenost jednotlivých částí eJustice navzájem a zároveň s ostatními částmi e-Governmentu. V 21. století se dle mého názoru stala justice z pohledu elektronizace obrovským a složitě propojeným informačním systémem, bez kterého by při současném počtu zahájených a běžících řízení, nebylo možno vyhovět oprávněnému zájmu na rychlém ale i efektivním rozhodování. Lze tedy konstatovat, že e-Government v justici má za úkol jak naplňovat ústavní právo na

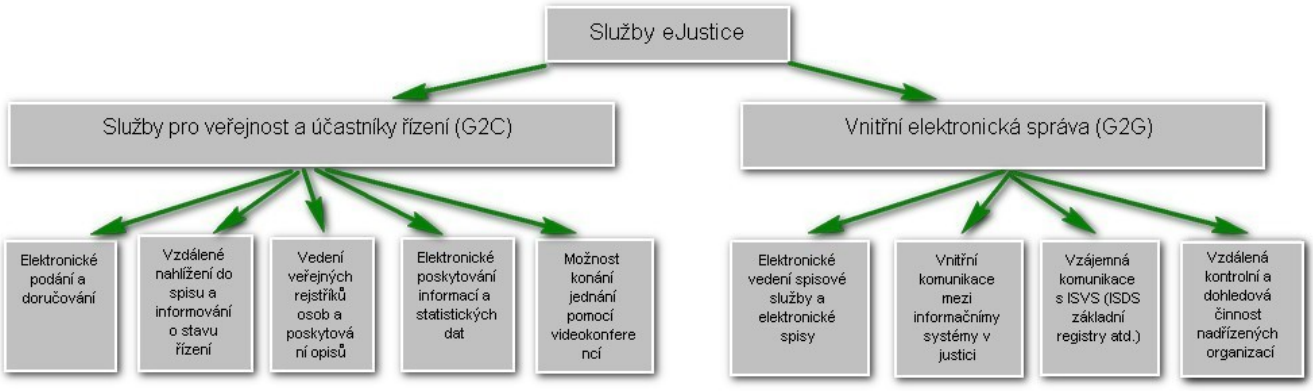
[37] ŠTĚDROŇ, Bohumír a Iva HŘEBÍKOVÁ. *Občanské soudní řízení sporné a využití informačních technologií a právních informačních systémů: (e-justice)*. 1. vyd. Praha: Linde, 2008, s. 15.

projednání věci bez zbytečných průtahů, tak, jak předpokládá čl. 38 odst. 2 Listiny, tak i pomáhat k zákonnému rozhodování tím, že poskytne možnost získat správné informace důležité pro rozhodnutí. Zejména v soudním řízení pak eGovernment úzce souvisí i s principy veřejnosti, tak jak jej předpokládá čl. 96 odst. 2 Ústavy, čl. 38. odst. 2. Listiny a § 116 odst. 1 o.s.ř. a rovněž princip hospodárnosti, který „*vyjadřuje požadavek, aby ochrana práv byla poskytnuta rychle, účinně a bez zbytečných nákladů.*“[38]

Informační systémy v justici pomáhají v evidenci téměř veškerých úkonů, které se provedou. Ať již jde o evidenci došlého podání či rozhodnutí ve věci, vytvoření a vypravení rozhodnutí či následného sledování jeho doručení. V justici se pracuje se značným množstvím informací, které je třeba získávat za účelem rozhodování ve věci a dnes již není možné se spoléhat na listinné žádosti zasílané jiným orgánům veřejné moci. Rovněž veřejnost, ale i informační systémy veřejné správy (např. ISDS či základní registry), potřebují pro své fungování informace, které získávají právě z oblasti justice.

Stejně jako eGovernment i eJustici lze členit na část, v rámci které dochází ke komunikaci s občany (v případě justice typicky s účastníky řízení) a na část, v rámci které dochází ke komunikaci s ostatními orgány veřejné moci.

Obrázek č. 6: Kategorizace služeb eJustice



Pramen: Vytvořeno autorem

[38] WINTEROVÁ, Alena a Alena MACKOVÁ. *Civilní právo procesní: vysokoškolská učebnice*. 7. aktualiz. a dopl. vyd. Praha: Linde, 2014, s. 71

Mezi základní cíle a poslání eJustice lze zařadit:

1. Zajistit podmínky pro transparentní, rychlé a zákonné rozhodování organizací justice.
2. Umožnit snadnou a přívětivou komunikaci s účastníky řízení, veřejností a jinými orgány veřejné moci.
3. Plnit zákonné povinnosti v oblasti vedení veřejných rejstříků právnických a fyzických osob a insolvenčního rejstříku.

Tyto základní cíle lze blíže specifikovat takto:

Ad 1) **Zajisti podmínky pro transparentní a rychlé rozhodování organizací justice**:

- umožnit efektivní a uživatelsky přívětivé vedení spisové služby, které usnadní evidovat veškeré potřebné a relevantní údaje a automatizovat opakující se úkony,
- usnadnit získávání informací důležitých pro rozhodnutí ve věci z jiných agendových informačních systémů mimo justici,
- zajistit interní komunikaci mezi informačními systémy používanými v resortu justice s cílem rychlého zjištění informací potřebných pro činnost organizace, event. pro rozhodování ve věci,
- využívání elektronického spisu a s tím spojenou úsporu kancelářských potřeb a vyšší bezpečnost údajů obsažených ve spise,
- usnadnit organizacím hlídaní zákonných, soudcovských a jiných lhůt,
- usnadnit prověrkovou a dohledovou činnost v souladu se zákonem,
- umožnit dodržování zákonem stanovených postupů při rozdělování věcí mezi různé subjekty (např. rozdělování napadlých věcí podle rozvrhu práce dle ust. § 42 odst. 2 zákona o soudech, soudcích, přísedících a státní správě soudů a o změně některých dalších zákonů (zákon o soudech a soudcích), ustanovování obhájců podle ust. § 39 trestního řádu, ustanovování insolvenčních správců podle ust. § 25 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákona),
- znemožnit svévolné změny relevantních údajů o průběhu řízení (datum rozhodnutí, vypravení rozhodnutí, zaevidování opravného prostředku, atd.),
- umožnit snadnou protokolaci o průběhu jednání.

Ad 2) **Umožnit snadnou a přívětivou komunikaci s účastníky řízení, veřejností a jinými orgány veřejné moci**

- umožnit snadný příjem podání v elektronické podobě,

- umožnit intuitivní a uživatelsky přívětivé vyplňování některých podání v elektronické podobě,
- umožnit elektronické doručování rozhodnutí a jiných písemností,
- zajistit komunikaci s ostatními ISVS (datové schránky, základní registry) případně agendovými informačními systémy (centrální evidence obyvatel, evidence cizinců, atd.),
- umožnit konání jednání či výslechu prostřednictvím videokonference,
- veřejně poskytovat statistická data o činnosti organizací justice,
- zveřejňovat důležitá rozhodnutí, která mohou ovlivnit rozhodování soudů (judikatura),
- umožnit vzdálené nahlížení účastníků do elektronického spisu,
- umožnit zveřejnění kontaktních údajů o organizaci prostřednictvím internetu,
- umožnit dálkový přístup na elektronickou úřední desku,
- informovat účastníky řízení o stavu jejich řízení,
- umožnit placení soudních a správních poplatků přes internet.

Ad 3) **Plnit zákonné povinnosti v oblasti vedení veřejného rejstříku právnických a fyzických osob a insolvenčního rejstříku**

- umožnit nahlížet do veřejného či insolvenčního rejstříku přes internet,
- umožnit vydávání ověřených výpisů a opisů z veřejného a insolvenčního rejstříku,
- zajistit komunikaci s ostatními ISVS (datové schránky, základní registry), s obchodním věstníkem, atd.

Samozřejmě i pro oblast justice platí jak základní právní principy, jako princip legitimity, tak i právo na informace dle Listiny. Při zavádění elektronizace justice, zejména pak soudnictví, je však třeba mimo zmíněné ústavní principy a práva dbát i na další úzce související. Hlavním rizikem je možnost narušení práva na soudní ochranu a principu rovnosti stran před soudem, a to v případě, kdy jedna strana nemá možnost využívat informační technologie, čímž by ji mohl být odepřen přístup k soudu či by mohla být během řízení znevýhodněna. Další hrozbou je možnost narušení principu nezávislosti soudu a soudce, a to např. v případě zavedení takových informačních technologií, které znemožní pracovat se spisem dle uvážení soudce.

Co se týče institucionálního zajištění rozvoje e-Governmentu, tak přestože v oblasti eGovernmentu ve veřejné správě má hlavní slovo Ministerstvo vnitra ČR, u eJustice je hlavním garantem Ministerstvo spravedlnosti ČR, které v souladu s ust. § 118 a násl. zákona o soudech a soudcích vykonává nad soudy státní správu, která samozřejmě nesmí zasahovat do

nezávislosti soudů. Hlavním zákonným ustanovením umožňujícím ministerstvu rozvíjet informační systémy soudů, je ust. § 123 odst. 1 písm. m) zákona o soudech a soudcích, podle kterého ministerstvo „*usměrňuje a řídí využívání informačních technologií*." Totožné ustanovení obsahuje i zákon č. 283/1993 Sb., o státním zastupitelství.[39]

Co se týká oblasti justice, neexistuje právní předpis, který by definoval či rámcově upravil využívání elektronických informačních systémů či obecně e-Governmentu v dané oblasti. Právní úprava je obsažena v zákonech a podzákonných předpisech uvedených v podkapitole 1.4, jejichž ustanovení jsou pak zohledněna v množství jiných právních předpisů. V oblasti justice jde zejména o procesní předpisy, kterými se soudy, státní zastupitelství a Probační a mediační služba řídí. Konkrétně jde o o.s.ř., trestní řád, soudní řád správní, ale i správní řád, které obsahují v návaznosti na základní zákony eGovernentu úpravu týkající se zejména příjmu podání v elektronické podobě, úpravu doručování, která byla podstatně upravena v návaznosti na zákon o datových schránkách nebo využívání údajů ze základních registrů.
Rovněž podzákonné předpisy, ať již obecně závazné nebo mající povahu interní instrukce, vydávané Ministerstvem spravedlnosti, obsahují ustanovení, která mají za cíl v rámci zákonného zmocnění upravit podmínky pro co největší využití nástrojů eJustice. Tyto jsou uvedeny v příloze č. 1.

3.1 Podání v elektronické podobě v justici

Jak bylo uvedeno, snadná a uživatelsky přívětivá komunikace s účastníky, veřejností a ostatními orgány veřejné moci je jedním z hlavních cílů eJustice, stejně jako celého eGovernmentu. Soudy, státní zastupitelství, vězeňská služba, Probační a mediační služba a Justiční akademie (dále jen „organizace") mají povinnost přijímat podání v elektronické podobě. Tato povinnost vyplývá z již zmíněných procesních předpisů, a to:

- § 42 odst. 1 o. s. ř,
- § 59 odst. 1 trestní řád,
- § 37 odst. 2 zákona č. 150/2002 Sb., soudní řád správní,
- § 37 odst. 4 zákona č. 500/2004 Sb., správní řád.

[39] Ust. § 13d písm. m) zákona č. 283/1993 Sb., o státním zastupitelství

Tyto zákony jednotně upravují možnost činit písemná podání v elektronické podobě. Tomu odpovídá povinnost uvedených orgánů tato podání přijímat. Elektronická komunikace s organizacemi justice je však zásadně fakultativní, a to až na několik výjimek:

1. Obecná povinnost daná ust. § 17 odst. 1 zákona o DS, dle které orgán veřejné moci musí doručovat jinému orgánu veřejné moci do datové schránky, umožňuje-li to povaha dokumentu,
2. Povinnost podávat návrhy na vydání elektronického platebního rozkazu na elektronickém formuláři dle § 174a odst. 1 o. s .ř.,
3. Povinnost exekutorů podávat návrh na pověření a nařízení exekuce ust. dle § 43a odst. 3 zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) v elektronické podobě.

Na organizace justice, jakožto na veřejnoprávní původce dle zákona o archivnictví, se vztahuje mimo jiné vyhláška č. 259/2012 Sb., která ukládá již zmíněnou povinnost přijímat datové zprávy učiněné na elektronické adresy (e-mail), prostřednictvím datových schránek a na technickém nosiči dat. Zároveň však umožňuje, aby si veřejnoprávní původce vybavil podatelnu i pro příjem jiných datových zpráv.

Lze říci, že počet podání v elektronické podobě v justici neustále roste, a to stále se zrychlujícím tempem. Na růstu podání má podíl jak rozšiřující se počítačová gramotnost veřejnosti, tak i legislativní kroky v nedávné době. Jde zejména o nabytí účinnosti zákona o DS, čímž vznikla povinnost orgánů veřejné moci komunikovat mezi sebou prostřednictvím datových schránek. Dále byly datové schránky povinně zřízeny většině právnických osob. Od 1. 7. 2012 skončila výjimka pro advokáty, kteří rovněž musí mít zřízenou datovou schránku. Přestože ani právnické osoby ani advokáti či insolvenční správci nemají povinnost komunikovat s organizacemi justice elektronicky, tuto možnost stále častěji využívají. Zasílání podání v elektronické podobě je bezesporu pro podatele výhodné z časových, ale i finančních důvodů. Jako hlavní výhody lze označit:

- podání je možné organizaci zasílat 24 hodin denně, 7 dní v týdnu; podatelé tak mají větší možnost využívat procesní a hmotněprávní lhůty, téměř až do „poslední vteřiny“,
- téměř nulové transakční náklady, kdy jediný výdaj je pro některé typy datových zpráv a některé typy podání pouze obligatorní kvalifikovaný certifikát, který je třeba každoročně

obnovovat; u datových schránek je pak komunikace vůči organizacím justice zcela zdarma; odpadají tak náklady za poštovné, obálky, papír, atd.,

- podatel je o doručení své datové zprávy bezprostředně informován, s čímž souvisí i možnost podatele doručení svého podání snadno doložit.

V roce 2013 bylo všem organizacím justice zasláno celkem 6,765.088 datových zpráv. Z toho bylo 6,283.107 datových zpráv zasláno soudům a 386.961 pak státním zastupitelstvím.

Z důvodu složitosti postupu při příjmu a následném zpracování datových zpráv vydalo Ministerstvo spravedlnosti závazný vnitřní pokyn, a to instrukci č. 133/2012-OD-ST, kterou se upravuje jednotný postup podatelny při příjmu a ověřování datových zpráv a dokumentů v nich obsažených. Instrukce nabyla účinnosti 1. 7. 2013 a platí pro všechny organizace. Tato instrukce jednak upřesňuje a doplňuje povinnosti stanovené ve vyhlášce č. 259/2012 Sb., a dále stanoví jednotná vnitřní pravidla při zpracování datových zpráv tak, aby výsledky při ověřování byly u všech organizací v justici jednotné.

Pro přehlednost, jednotnost a srozumitelnost zavedla instrukce rovněž povinnost všech organizací zveřejnit na svých internetových stránkách a úřední desce jednotnou informaci o příjmu podání v elektronické podobě, která je pro všechny stupně organizací až na drobnosti nyní stejná. Došlo tak k nahrazení informací o příjmu podání jednotlivých organizací, které byly v různé kvalitě, někdy i v rozporu s právními předpisy.

3.1.1 Typy přijímaných datových zpráv a datové formáty dokumentů

Zákonnou povinnost přijímat podání v elektronické podobě lze snadno „obejít“ tím, že organizace bude klást velké a nesmyslné nároky na náležitosti datové zprávy či dokumentu (např. povinnost používat málo rozšířené datové formáty atd.). Lze konstatovat, že toto není případ justice, která nejenže přijímá v souladu s vyhláškou č. 259/2012 Sb. datové zprávy zaslané na elektronické adresy (e-mail) a datovou schránkou, ale nad minimální rámec vyhlášky, a v souladu s instrukcí č. 133/2012-OD-ST, přijímá ještě další dva typy datových zpráv, a to:

1. Již od 1. 10. 2007 je se soudy možné komunikovat prostřednictvím webové aplikace ePodatelna, která je dostupná ze stránek www.justice.cz. Jde o jeden z prvních nástrojů elektronické komunikace prostřednictvím internetových stránek. Prostřednictvím dané aplikace je možné soudu podávat veškerá podání v elektronické podobě (žaloby, návrhy na zahájení řízení, opravné prostředky, atd.). Podatel však vždy musí datovou zprávu podepsat elektronickým podpisem.

2. Na stránkách webové aplikace ePodatelny jsou rovněž vystaveny některé typy PDF formulářů, které lze považovat za datovou zprávu. V současné době jde o formulář návrhu na vydání elektronického platebního rozkazu, formulář přihlášky pohledávky do insolvenčního řízení, formulář žádosti exekutora o pověření k provedení exekuce a formuláře určené pro notáře. Všechny tyto formuláře lze po jejich podepsání elektronickým podpisem přímo odeslat (stisknutím tlačítka „Odeslat“ na konci formuláře), aniž by bylo nutné je připojovat k jiné datové zprávě (e-mail, datová schránka, webová ePodatelna). Tyto formuláře tak tvoří datovou zprávu samy o sobě a zároveň jsou i podáním v elektronické podobě.

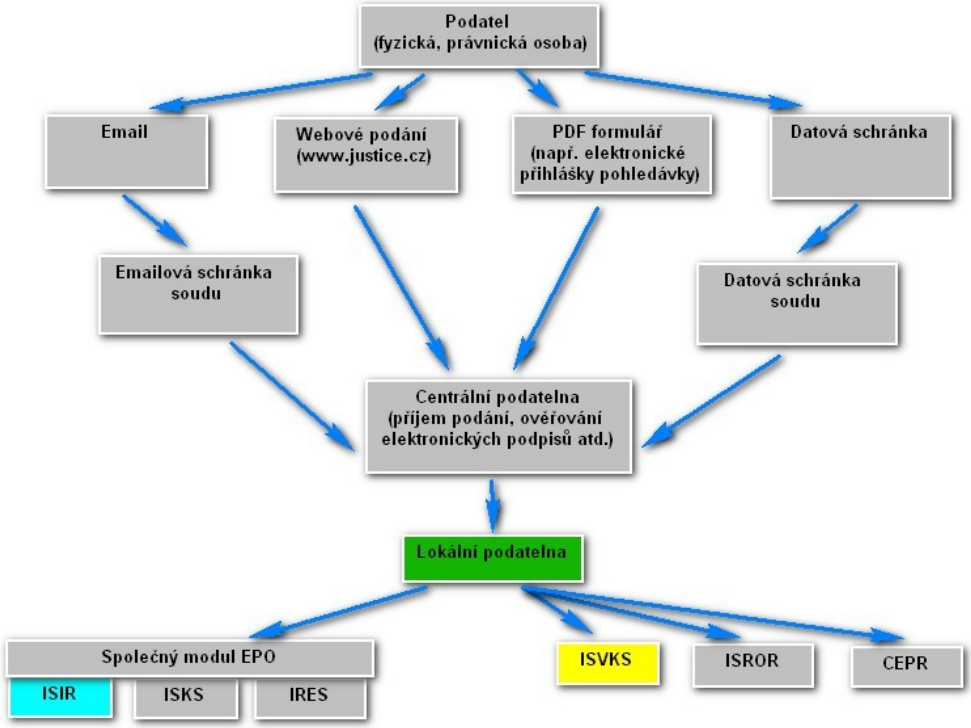
Co se týče přijímaných datových formátů dokumentů, tak v souladu se zákonem o archivnictví přijímají organizace povinné formáty, tedy PDF, PNG, TIF, TIFF, JPEG/JFIF, MPEG-2, MPEG-1, GIF, MP2, MP3, WAV a PCM. Nadto stanovila instrukce č. 133/2012-OD-ST povinnost všem organizacím přijímat i další časté textové formáty, a to DOC, DOCX, TXT, RTF, XLS, XLSX a ZFO. Důvodem je usnadnit podatelům komunikovat v běžných datových formátech dokumentů. Jednotlivé organizace si mohou stanovit i další přijímané formáty, v praxi se tak však neděje.

Jako sporné se jeví přijímání podání na technických nosičích dat. Podle vyhlášky č. 259/2012 Sb., by měly organizace justice tyto nosiče přijímat, procesní předpisy v justici však takové podání neumožňují, když např. o. s. ř. ve svém ust. § 42 odst. 1 stanoví, že podání v elektronické podobě se činí prostřednictvím veřejné datové sítě. Odlišná situace však dle mého názoru platí pro přílohy k podání (důkazy), které by organizace justice přijímat na technických nosičích dat měly. V tomto smyslu hovoří i ust. § 6 odst. 2 instrukce 133/2012-OD-ST.

3.1.2 *Technické řešení podatelny a zpracování datových zpráv a dokumentů v nich obsažených*

Aby byla zachována jednotnost při příjmu datových zpráv a zároveň odpovídající zabezpečení datové sítě, zvolilo Ministerstvo spravedlnosti řešení jednotného informačního systému elektronické podatelny, který je tvořen centrální částí a lokálními částmi, která jsou na všech soudech, státních zastupitelstvích a střediscích Probační a mediační služby. Obě části jsou pak spravovány Ministerstvem spravedlnosti a dodávány externím dodavatelem. Centrální část (tzv. CEPO – Centrální podatelna) zejména zajišťuje příjem datových zpráv, odesílání potvrzení o příjmu datové zprávy, antivirovou a antispamovou kontrolu a na základě nastavení jednotlivých organizací i kontrolu elektronických podpisů, značek a časových razítek jak u samotných datových zpráv, tak i u vložených dokumentů. Následně v lokální části, která je nainstalována na všech podatelnách organizací, probíhá zpracování datové zprávy a dokumentů pracovníky podatelny. Jde zejména o tisk podání, případně ruční ověřování podpisů a následné přiřazení podání do příslušného informačního systému.

Obrázek č. 7. Struktura informačních systémů přijímajících elektronická podání pro krajské soudy



Pramen: Vytvořeno autorem

Předmětem sporu v justici byl rozhodný okamžik zahájení soudního řízení v situaci, kdy mezi odesláním datové zprávy a jejím doručením do faktické dispozice soudu (tedy až do lokální podatelny) byl dlouhý časový interval. Nakonec bylo zaujato všeobecně přijaté stanovisko, že okamžikem doručení datové zprávy je okamžik, kdy je doručeno do e-mailové či datové schránky soudu a u webových a formulářových podání je to okamžik doručení do centrální podatelny. Obecně tedy okamžikem doručení není až dodání do lokální podatelny, což však příliš neodpovídá ust. § 3 odst. 1 vyhlášky 259/2012 Sb. Nicméně jsem toho názoru, že podateli nemůže jít k tíži časová prodleva mezi okamžikem, kdy ztratí dispozici s datovou zprávou (tedy jejím odesláním) a okamžikem, než se podání dostane do podatelny. Jistě však bude zajímavé, jak bude soudem řešena situace, kdy podatel odešle datovou zpráv datovou schránkou, ale z důvodu výpadku či přetížení ISDS se datová zpráva dodá do datové schránky soudu až např. za několik hodin.

Informační systém elektronické podatelny v současné době splňuje všechny podmínky dané vyhláškou č. 259/2012 Sb. i vyhláškou č. 212/2012 Sb. (ověřování vůči předepsanému seznamu zneplatněných certifikátů, vyhodnocování podpisů s přihlédnutím k okamžiku přiložení časového razítka atd.).

O ověření každé datové zprávy je v souladu s ust. § 6 odst. 4 vyhlášky č. 259/2012 Sb. tvořen záznam o ověření datové zprávy a dokumentů v ní obsažených, běžně nazývaný jako identifikátor. Vzor tvoří přílohu č. 2. Identifikátor obsahuje údaje o typu podání, okamžiku jeho dodání, o odesílateli a o výsledku ověřování podpisů a značek. Jde v podstatě o podací razítko elektronického podání (viz ust. § 2 odst. 4 písm. b) zrušené vyhlášky 496/2004 Sb. a nyní ust. § 10 odst. 1 instrukce 133/2012-OD-ST) a je spolu s podáním zakládáno do spisu. Na základě identifikátoru pak příslušný pracovník soudu (soudce, vyšší soudní úředník, asistent soudce) vyhodnotí, zda bylo podání zasláno včas, oprávněnou osobou a zda je řádně podepsáno, pokud to zákon vyžaduje.

O doručení datové zprávy musí být podatel vyrozuměn, a to v souladu s ust. § 6 odst. 3 vyhlášky č. 259/2012 Sb. Rovněž musí být vyrozuměn o výsledku ověřování elektronických podpisů. Nadto vyhláška stanoví povinnost vyrozumět podatele i v případě, kdy je dokument poškozen, je v nepovoleném datovém formátu či obsahuje škodlivý kód. V případě e-mailů, webové ePodatelny a formulářových podání odesílá tyto informace automaticky informační

systém centrální elektronické podatelny. Ruční informování je při počtu došlých datových zpráv naprosto vyloučeno. Výše uvedené povinnosti ovšem platí pouze v případě, kdy je organizaci známa elektronická adresa odesílatele. Neplatí to tedy pro podání učiněná datovou schránkou, kde potvrzení o doručení datové zprávy tvoří přímo ISDS. Pokud je však dokument došlý datovou schránkou poškozen či v nepovoleném datovém formátu, musí vyrozumívat podatele pracovník podatelny.

3.1.3 Elektronické podpisy a jejich ověřování v justici

Jedním z nejdůležitějších ustanovení stanovujícím povinnost podepisovat podání vůči soudu je ust. § 42 o. s. ř. Podle odst. 1 je možné podání činit písemně v listinné či elektronické podobě. Od 1. 1. 2014 došlo k několika upřesňujícím změnám, které však působí podle mého názoru poněkud kostrbatě. Podle ust. § 42 ost. 2 o. s. ř. „*písemné podání obsahující návrh ve věci samé učiněné telefaxem nebo v elektronické podobě je třeba nejpozději do 3 dnů doplnit předložením jeho originálu, případně písemným podáním shodného znění. K těmto podáním, pokud nebyla ve stanovené lhůtě doplněna, soud nepřihlíží.“* Podle odst. 3 „*v případě podání v elektronické podobě podepsaného uznávaným elektronickým podpisem nebo podání v elektronické podobě podle zvláštního právního předpisu se nevyžaduje doplnění podání předložením jeho originálu podle odstavce 2.“* Podle odst. 4 věta první platí, že „*pokud zákon pro podání určitého druhu nevyžaduje další náležitosti, musí být z podání patrno, kterému soudu je určeno, kdo je činí, které věci se týká a co sleduje, a musí být podepsáno a datováno. Povinnost podpisu a datování se nevztahuje na podání v elektronické podobě podle zvláštního právního předpisu.“* Podle věty poslední „*k podání učiněnému elektronicky lze připojit také všechny jeho přílohy v elektronické podobě.“*

Zákona tedy stanoví povinnost podepisovat elektronickým podpisem pouze podání ve věci samé (žaloby, návrhy na zahájení řízení, opravné prostředky, atd.), ale nic nehovoří o nutnosti podepisovat přílohy k podání v procesním slova smyslu (např. plnou moc pro zástupce atd.)

Největší změnou oproti dosavadní úpravě ust. § 42 o. s. ř. je výslovné uvedení, že v případě podání učiněné datovou schránkou nemusí být datová zpráva (dokument) podepsán elektronickým podpisem. Jde o výslovné promítnutí ust. § 18 odst. 2 zákona o DS, který fakticky zavádí fikci podpisu, a podle kterého „*úkon učiněný osobou uvedenou v § 8 odst. 1 až 4 nebo pověřenou osobou, pokud k tomu byla pověřena, prostřednictvím datové schránky má*

stejné účinky jako úkon učiněný písemně a podepsaný, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob.“ Obdobným způsobem bylo upraveno ust. § 97 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), který upravuje podepisování insolvenčního návrhu a rovněž ust. § 22 odst. 3 zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob (dále jen „zákon o veřejných rejstřících“).

Jde o reakci na rozdílné právní názory v justici, kdy existovaly dva různé výklady. Podle RNDr. Peterky a Mgr. Podaného, kteří patří k nejhlasitějším odpůrcům fikce podpisu v justici, jde o nevhodnou anomálii, která může vytvářet konflikt se zvláštními právními předpisy, které podpis vyžadují. Dalším důvodem je, že nepodepsaný dokument znemožňuje autorizovanou konverzi. Rovněž možnost snadného ověření, zda dokument poslala oprávněná či pověřená osoba (§ 8 zákona o DS) v případě absence elektronického podpisu chybí, protože ne vždy je možné zjistit, zda odesílající osoba má skutečně oprávnění za držitele datové schránky v konkrétní věci jednat. V ISDS byla informace o konkrétní odesílající osobě zapracována až v průběhu ostrého provozu a stále je nepovinná a nemusí být u datové zprávy obsažena. Dle názoru výše uvedených autorů je tedy nutno fikci podpisu dovozovat ve vztahu k oprávněné či pověřené osobě, která konkrétní podání vůči organizaci justice učinila. V podobném smyslu se vyjádřil i Nejvyšší správní soud v rozhodnutí č. j. 8 As 89/2011 – 31 ze dne 17. 2. 2012.

Naopak Ministerstvo spravedlnosti zastávalo opačný názor, který se dá stručně shrnout tak, že je na držiteli datové schránky, jak si sám zařídí přístupy jednotlivých osoba do datové schránky a jaká jim zřídí oprávnění. Elektronický podpis tedy není potřeba. Tento názor je od 1. 1. 2014 výslovně demonstrován v uvedených ustanoveních procesních předpisů.

Možnou absenci elektronického podpisu však nelze brát absolutně. Např. pokud je podání zasíláno typicky z datové schránky advokáta zastupujícího podatele na základě plné moci, je nutno přiložit plnou moc podepsanou klientem. Plná moc pak musí být buď podepsána elektronických podpisem klienta, nebo být autorizovaně konvertována. Tato povinnost je výslovně uvedena v § 97 odst. 2 insolvenčního zákona, platí však dle mého názoru pro jakýkoliv typ řízení.

3.1.4 Aktuální sporné otázky a praktické problémy při příjmu datových zpráv

Vedle výše popsané problematiky týkající se nutnosti připojení elektronického podpisu k datové zprávě doručované datovou schránkou, jsou s příjmem datových zpráv a dokumentů spojeny i mnohé další praktické problémy, které bych zmínil v několika bodech:

Vysoké finanční náklady

S pořízením, údržbou a případným zlepšováním funkčnosti informačního systému el. podatelny jsou spojeny značné finanční náklady. Jsem toho názoru, že by Ministerstvo vnitra ČR, v souladu se zákonem o ISVS, mělo vytvořit a poskytnout všem orgánům veřejné moci jednotný informační systém elektronické podatelny splňující veškeré legislativní nároky, které ostatně původně vzešly právě od Ministerstva vnitra ČR. Eventuálně by mělo alespoň poskytnout doporučenou metodiku pro nastavení informačního systému elektronické podatelny.

Nedostatečná legislativní úprava

V justici již delší dobu probíhá debata týkající se otázky, zda pro relevanci datové zprávy odeslané na elektronickou adresu (e-mail) musí být podepsána zároveň samotná datová zpráva (tělo e-mailu) a současně přiložené dokumenty, případně postačuje podepsat pouze buď datovou zprávu, anebo přímo daný dokument. Odpověď je dle mého názoru třeba odvíjet primárně od skutečnosti, zda je vlastní podání obsaženo přímo v datové zprávě (tělo e-mailu) nebo tvoří přílohu (vložený dokument) této zprávy. Obvykle v těle e-mailu jsou uvedeny pouze průvodní informace, kterými odesílatel sděluje, že v příloze (dokumentu) je obsaženo vlastní podání. K tomuto zdánlivě banálnímu problému ovšem existuje četná judikatura, která však často obsahuje rozporuplné závěry. RNDr. Peterka a Mgr. Podaný prezentují názor, že je třeba, aby byl zejména podepsán dokument obsahující podání, samotná datová zpráva být podepsána nemusí. Osobně se mi jeví tento názor jako nadměrný formalismus ve vztahu k podatelům. V tomto smyslu rozhodl i Ústavní soud v usnesení sp. zn. II. ÚS 3042/12, kde připustil, že „*elektronický podpis zprávy jako celku identifikuje toliko autora e-mailu a neosvědčuje již autorství odesílatele ve vztahu k přílohám, nelze ovšem přehlédnout, že autorství není, snad jen s výjimkou vlastnoručně sepsaného podání, s jistotou určitelné ani u písemného podání. Ve vztahu k přílohám je nicméně možno podpis zprávy chápat ve smyslu:*

"jsem ten, kdo vložil tyto přílohy", tj. potvrzuje vůli autora e-mailu odeslat do podatelny soudu připojené dokumenty, s nimiž se, implicitně vzato, ztotožňuje. Je jistě v zájmu právní jistoty účastníků řízení žádoucí, aby opatřili zaručeným elektronickým podpisem také samotné podání, a nikoliv pouze průvodní email, na druhou stranu s nedodržením tohoto postupu nelze spojovat následek spočívající v odepření soudní ochrany." Obdobně rozhodl Ústavní soud i v nálezu IV. ÚS 1829/13 ze dne 12. 2. 2014. V praxi existují další eventuality, které nejsou dostatečně legislativně upraveny, např. když podpis těla emailu patří jiné osobě než podpisy dokumentů, či podepsané tělo emailu obsahuje část podání a zbylá část je v přiloženém dokumentu, který je nepodepsaný atd. Praxe je v tomto směru opravdu bohatá.

Dále není legislativně upraveno, jak nahlížet na datovou zprávu či dokument, který je podepsán elektronickým podpisem založeným na kvalifikovaném certifikátu, kterému vypršela platnost. Vyhláška č. 212/2012 Sb. tuto situaci neřeší. Dle stanoviska Ministerstva vnitra *„skutečnost, že kvalifikovaný certifikát, na kterém je založen zaručený elektronický podpis, jímž je podepsán dokument obsažený v datové zprávě, pozbude platnosti tokem času (expiruje), nemá vliv na platnost zaručeného elektronického podpisu, a tedy ani na pravost dokumentu. Uvedené platí i v případě elektronické značky a kvalifikovaného časového razítka."*[40]

V návaznosti na předešle uvedené skutečnosti lze konstatovat, že existují 3 možné výsledky vyhodnocování platnosti el. podpisu.

1. podpis je platný,
2. podpis je neplatný,
3. podpis nelze ověřit.

A právě v případě, kdy certifikátu uplynula doba platnosti (a platnost elektronického podpisu nebyla prodloužena časovým razítkem) je nutno konstatovat, že nelze elektronický podpis ověřit. S tím se však hlavně u podání ve věci samé nelze pro další postup v řízení smířit. Instrukce č. 133/2012-OD-ST pro tento případ stanoví povinnost vyrozumět podatele o tom, že na jeho podání se bude nahlížet, jakoby nebylo podepsáno, nicméně jde pouze o vnitřní pokyn, který v případě sporu nemusí být brán jako argument dostatečné síly.

[40] č. j. MV-36491-1/AS-2010 ze dne 6.4.2010

V českém právním řádu dále zcela absentuje úprava postupu při ověřování datové zprávy či častěji dokumentů, které jsou podepsány více elektronickými podpisy. Jednotlivé podpisy mohou mít mezi sebou různý vztah, mohou být paralelní, kde není důležité pořadí podpisů, ale mohou být např. zaobalovací, kde poslední podpis stvrzuje, že dokument byl před třetí osobou podepsán (typicky notářské zápisy). V tomto případě je důležitá posloupnost podpisů. Rovněž mohou nastat situace, kdy je jeden či více podpisů na dokumentu neplatných (např. z důvodu porušení integrity dokumentu) zatímco jeden (či více) jsou naopak platné. Lze považovat takový dokument za podepsaný platným podpisem a za jakých situací?

Datové zprávy a dokumenty lze různým způsobem šifrovat či zaheslovat. Pokud je takový dokument doručen orgánu veřejné moci, je otázkou, zda jej lze považovat za doručený, pokud organizace justice nemá k dešifrování prostředky či nezná heslo. Dle mého názoru lze na takovou datovou zprávu či dokument nahlížet jako na dokument, který nelze zobrazit uživatelsky vnímatelným způsobem, tak jak to definuje ust. § 3 odst. 1 vyhlášky č. 259/2012 Sb.

Zákon o elektronickém podpisu umožňuje v ust. § 12 odst. 1 písm. c) vydat kvalifikovaný certifikát, ve kterém je osoba označena pseudonymem. Podle ust. § 17 zákona o elektronickém podpisu sice musí být z certifikátu toto jednoznačně patrné, nicméně vyvstává otázka, zda organizace justice může považovat takovéto podání za podepsané, když se nemůže spolehnout na údaje z certifikátu. Skutečnou identitu podepisující osoby zná pouze certifikační autorita. Má organizace povinnost „pátrat“ po podepisující osobě (což může být zvlášť problematické u podání typu insolvenčního návrhu či návrhu na vydání předběžného opatření) či může považovat takové podání za nepodepsané? Dle mého názoru není povinností organizace zjišťovat pravou totožnost podepisující osoby a na takové podání by měla nahlížet jako na nepodepsané. Takto je to rovněž upraveno v ust. § 15 instrukce č. 133/2012-OD-ST.

Kvalifikovaný certifikát, jak vyplývá z jeho definice uvedené v ust. § 11 odst. 3 zákona o elektronickém podpisu, musí obsahovat údaje, které jednoznačně umožní identifikaci podepisující osoby. Vyhláška č. 212/2012 Sb., převzala z vyhlášky č. 496/2004 Sb. ustanovení o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, což vyplývá z ust. § 20 odst. 4 zákona o elektronické podpisu. Mělo by jít o desetimístné číslo. Stanovisko Ministerstva vnitra ČR je v tomto případě značně

benevolentní, neboť dle jejich domněnky „*bude vhodné i nadále využívat jako tyto údaje právě identifikátor klienta Ministerstva práce a sociálních věcí, neboť ten splňuje požadavky vyhlášky č. 212/2012 Sb., je vybudována komunikační infrastruktura, jsou zavedeny postupy pro jeho přidělování a na práci s tímto identifikátorem jsou konfigurovány informační systémy orgánů veřejné moci*.“[41] Není tak vůbec dořešeno, jak se takový identifikátor má získat a co dělat s certifikáty, které jej neobsahují.

Rozhodnutí Komise 2009/767/ES byla stanovena povinnost přijímat i podání opatřená elektronickým podpisem, jež vznikl na základě certifikátu vydaného poskytovatelem na území EU. Dostupná aplikace pro ověřování vydavatele certifikátu nám však pouze řekne, zda se jedná o správného vydavatele, ale nic neřekne o platnosti podpisu. Je tedy otázkou, jak má orgán veřejné moci s takovým podáním naložit, když není schopen ověřit platnost elektronického podpisu.

Praktické problémy při zpracování datových zpráv

S příjmem podání v elektronické podobě jsou spojeny i problémy, které jsou sice legislativně upraveny, ale způsobují praktické problémy při jejich zpracování.

Často se stává, že výhoda pro podatele, která spočívá v možnosti zaslat podání „na poslední chvíli“ je velkou nevýhodou pro organizace justice. Je již zavedenou praxí, kdy zejména advokáti zasílají svá podání, včetně omluv z jednání, na poslední chvíli a podatelna nemá možnost taková podání včas zpracovat a předat příslušnému úseku soudu či státního zastupitelství. To pak může mít závažné důsledky např. při rušení rozsudků pro zmeškání[42], atd.

Vyhláška č. 212/2012 Sb. stanoví, že pokud je k ověření platnosti podpisu použit seznam zneplatněných certifikátů (což v daném případě v justici je vždy), je nutno platnost podpisu ověřovat proti CRL seznamu, který byl vydán 24 hodin od okamžiku, ke kterému je platnost podpisu ověřována, tedy od doručení datové zprávy soudu. Z toho plyne, že platnost či

[41] Stanovisko Ministerstva vnitra [online]. Vydáno 15.9.2012 [cit. 1.3.2014]. Dostupné z: <http://www.mvcr.cz/clanek/stanovisko-k-problematice-udaju-umoznujicich-jednoznacnou-identifikaci-podepisujici-osoby.aspx>

[42] viz ust. § 153b odst. 1 o. s. ř.

neplatnost podpisu může organizace justice s jistotou určit až po 24 hodinách. Opět toto činí problémy u podání typu insolvenčních návrhů či předběžných opatření, kde jsou velice krátké lhůty k prvním úkonům ve věci. Praxe je taková, že organizace justice nečekají 24 hodin na zpracování podání. Informační systém elektronické podatelny však sleduje případné dodatečné zneplatnění certifikátu, a pokud se tak stane, vyrozumí o tom příslušnou organizaci e-mailem. Je však otázkou, jak postupovat, pokud již bylo ve věci nějakým způsobem rozhodnuto.

Ne vždy se podaří ověřit podpisy na všech datových zprávách a dokumentech. Důvodem mohou být jednak technické problémy informačního systému, a jednak některé dosud nedopracované funkčnosti. V těchto případech musí organizace ověřovat podpisy atd. „ručně“, kdy musí pracovník podatelny sám ověřit, zda je elektronický podpis založen na kvalifikovaném certifikátu vydaným akreditovaným poskytovatelem certifikačních služeb a dále musí z internetových stránek jednotlivých poskytovatelů ověřit platnost certifikátu. Tento postup je nejen relativně zdlouhavý, ale i metodicky složitý. Postup ověřování platnosti elektronického podpisu je uveden v příloze č. 3.

Závěrem uvádím již jen „méně závažné“ problémy spojené zejména s „lidovou tvořivostí“ některých podatelů. Není výjimkou, kdy je např. několik podání týkajících se různých řízení naskenováno do jednoho elektronického dokumentu, což způsobuje problémy při jeho zpracování. Dále se objevují případy, kdy je návrh na vydání elektronického platebního rozkazu vytištěn, oskenován a zaslán např. e-mailem, což samozřejmě neumožní přenést automaticky z návrhu jakékoliv údaje do informačního systému. Těchto eventualit je však velké množství.

3.2 Datové schránky a elektronické doručování účastníkům v justici

Justici lze považovat za oblast, v níž dochází četnému využívání služeb datových schránek. Propojení justice s datovými schránkami lze rozdělit do 3 okruhů:

1. Příjem datových zpráv doručených prostřednictvím datových schránek (viz předchozí kapitola).
2. Odesílání datových zpráv orgány justice prostřednictvím datových schránek.

3. Vyrozumívání ISDS o zápisu právnické osoby do obchodního rejstříku (viz následující kapitola).

3.2.1 Doručování do datové schránky účastníka

U doručování soudů a státních zastupitelství účastníkům řízení lze konstatovat, že justice je jedním z největších odesílatelů datových zpráv v České republice. Procesní předpisy aplikované v justici byly zákonem č. 7/2009 Sb. novelizovány tak, aby byly v souladu se zákonem o DS. Jde zejména o ust. § 45 odst. 1 o.s.ř., které stanoví povinnost doručovat, pokud nedošlo k doručení při jednání či soudním úkonu, přednostně prostřednictvím veřejné datové sítě do datové schránky. Daná novela tak přinesla *„zákonné pořadí způsobů pro doručení s prioritou elektronické formy prostřednictvím datových schránek.“*[43] A teprve není-li to možné, nejčastěji protože adresát datovou schránku nemá nebo to zákon nepřipouští, je možné písemnost doručit na žádost adresáta na jinou adresu nebo na elektronickou adresu. Úprava obsažená v ust. § 62 odst. 1 trestního řádu je obdobná. V praxi tedy soud či státní zastupitelství musí před každým odesláním písemnosti (přípisu či rozhodnutí, apod.) provést kontrolu, zda osoba, které má být doručeno, nemá zřízenu datovou schránku, a pokud ano, zda je aktivní. Z důvodu obligatorní povinnosti doručovat do datové schránky a s tím spojenou možnost neplatného doručení, je nutné o každé kontrole evidovat tzv. „záznam o kontrole datové schránky“, který se automaticky ukládá do informačního systému soudu.

Podle ust. § 21b odst. 1 vyhlášky č. 37/1992 Sb. o jednacím řádu pro okresní a krajské soudy (dále jen „jednací řád“) *„soud vyhotovuje rozhodnutí a další písemnosti v té podobě, v jaké je veden spis. Opisy nebo stejnopisy rozhodnutí a dalších písemností se vyhotovují v listinné nebo v elektronické podobě podle způsobu doručování účastníkům nebo jiným osobám*.“ Každý stejnopis písemnosti v elektronické podobě, kterou soud doručuje účastníkům, se v souladu s ust. § 40b odst. 3 o. s. ř. podepisuje elektronickým podpisem toho, kdo stejnopis písemnosti vyhotovil. Nejčastěji jde o pracovníka soudní kanceláře (zapisovatelka či vedoucí kanceláře). Ale v případě, kdy se vydává originál rozhodnutí v elektronické podobě (nyní pouze u elektronických platebních rozkazů) podepisuje stejnopis elektronickým podpisem soudce či vyšší soudní úředník. Na písemnosti v elektronické podobě soud rovněž přidává časová razítka. Důvodem podepisování písemností a přidávání časového razítka je, aby měl

[43] KORBEL, Fratišek. Elektronická spravedlnost (2). *Právo & Byznys*. 2012, 1/2012, str. 25

účastník možnost si nechat dokument konvertovat, a to po dobu několika let. V době, kdy přidávání časových razítek neprobíhalo, se běžně stávalo, že si účastník neměl možnost konvertovat stejnopis rozhodnutí, a to z důvodu neplatnosti elektronického podpisu způsobeného zneplatněním certifikátu zaměstnance soudu, např. z důvodu skončení jeho pracovního poměru.

O. s. ř. rovněž v ust. § 46 odst. 2 umožňuje, aby soud doručoval písemnost účastníkovi e-mailem, a to v případě, kdy o to adresát požádá. Při doručování písemnosti emailem musí soud vyzvat adresáta, aby do 3 dnů od odeslání písemnosti potvrdil jejich přijetí. Toto potvrzení má být rovněž podepsáno uznávaným elektronickým podpisem. V praxi však tento způsob doručování písemností není příliš často využívaný.

Jako značným problém se v justici ukazuje zpětné znepřístupnění datové schránky, které může Ministerstvo vnitra ČR provést v souladu s ust. § 11 zákona o DS. „*Zpětně se datová schránka znepřístupňuje z toho důvodu, aby se negovalo doručení zpráv, které byly dodány do datové schránky, v době, kdy již osoba (fyzická nebo právnická) přestala existovat nebo byla omezena na osobní svobodě, ale Ministerstvo vnitra ČR ještě tuto informaci nedostalo a docházelo by např. k doručení písemností fikcí. Nelze, a to ani fikcí, doručovat osobě, která již neexistuje, nevykonává činnost, pro kterou byla datová schránka zřízena.*“[44] Pokud organizace justice doručovala do datové schránky osoby rozhodnutí a následně tato byla zpravomocněna, pak po zjištění, že byla zpětně znepřístupněna datová schránka, musí právní moc na všech neúčinně doručených rozhodnutích zrušit a doručovat je znovu. To je skutečný problém zejména v případě, kdy již např. probíhá výkon rozhodnutí či exekuce na splnění povinnosti uložené v neplatně doručeném rozhodnutí.

Za jednu z častých vad lze označit doručení písemnosti adresátu jiným způsobem než do datové schránky, pokud má datovou schránku zřízenu a zpřístupněnu. Organizace tedy z různých důvodů nedoručí písemnost do datové schránky, ačkoliv ji osoba má zřízenu a je aktivní. Další častou chybou je doručování rozhodnutí správné osobě, ale do nesprávného typu datové schránky. Dle jednoho z názorů „*ve všech těchto případech platí pravidlo materiality. Pokud adresát zásilku fakticky obdržel, považuje se zásilka za doručenou bez*

[44] SMEJKAL, V. *Datové schránky v právním řádu ČR. Zákon č.300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů s komentářem.* 1. vydání. Praha : ABF, a. s., 2009, s. 72,

ohledu na vady postupu, nemá-li forma zvítězit nad materiálním účelem doručování. Pokud adresát zásilku v důsledku vadného doručování fakticky neobdržel, doručena není a nemůže být doručena ani fikcí náhradního doručení uplynutím doby deseti dnů od uložení zásilky na poště či v datové schránce. Tento výklad zohledňuje účel doručování písemností, kterým je jak efektivita systému a zamezení obstrukcím, tak i ochrana legitimního očekávání osob a faktické seznámení se adresáta s doručovanou písemností.“[45]

3.2.2 Autorizovaná konverze v justici

Rovněž organizace justice, zejména soudy, provádějí autorizovanou konverzi dokumentů z moci úřední. Podle ust. § 23 zákona o DS provádí konverzi z moci úřední orgány veřejné moci pro výkon své působnosti. Ukázalo se však, že je v praxi zcela nereálné, aby se konvertovaly tisíce dokumentů došlých denně v elektronické podobě do listinné podoby a naopak. Bylo zaujato stanovisko, že zákon o DS neukládá povinnost konvertovat veškeré došlé dokumenty. Do jednacího řádu bylo proto vloženo ust. § 25 odst. 3, podle kterého „*vede-li se ve věci spis v elektronické podobě, soud převede podání a jiné písemnosti doručené v listinné podobě do elektronické podoby, kterou založí do elektronického spisu; autorizovaná konverze se neprovádí.“* Obdobné stanoví ust. § 25 odst. 4, podle kterého „*bylo-li podání nebo jiná písemnost doručena soudu jako součást datové zprávy, soud jej založí do elektronického spisu nebo převede do listinné podoby a založí do listinného spisu; autorizovaná konverze se neprovádí.“* Jednací řád upravuje i situace, kdy podání přijde v elektronické podobě od jednoho účastníka a následně se musí přeposlat v listinné podobě druhému účastníkovi a naopak. I zde se podle ust. § 28b odst. 2 a 3 autorizovaná konverze neprovádí.

Soud tak provádí konverzi ve výjimečných případech, např. když doručuje účastníkům do datové schránky rozhodnutí nadřízeného soudu, které obdržel spolu se spisem v listinné podobě. Stejně tak soud konvertuje z moci úřední např. v případě, kdy si účastník požádá o zaslání stejnopisu rozhodnutí v listinné podobě, když originál byl vytvořen v podobě elektronické (např. elektronický platební rozkaz).

[45] KORBEL, F., PRUDÍKOVÁ, D.: *Datové schránky tři roky poté: praktické zkušenosti s jejich používáním*, Bulletin advokacie č. 5/2012, str. 25.

3.3 Základní registry a agendové informační systémy a jejich využívání

Běžná činnost soudů a státních zastupitelství směřující k rozhodnutí se neobejde bez přístupu k informacím potřebným pro rozhodnutí ve věci. Tyto informace mohou být získány písemným dotazem na příslušný orgán veřejné moci, který rovněž většinou odpovídá písemně. S tím je spojena jak pracnost na obou stranách, tak finanční náklady, ale i prodlužování řízení. Proto je jedním z hlavních cílů eGovernmentu umožnit, aby si organizace justice samy mohly získat informace prostřednictvím přímého přístupu do příslušného agendového informačního sytému, nebo aby se jim informace přenášely do soudních informačních systémů zcela automaticky.

Mohlo by se zdát, že největším zdrojem informací pro soudy a státní zastupitelství budou, v souladu s jejich zákonným účelem, základní registry. Nicméně mimo soudy, které vedou veřejné rejstříky (viz podkapitola 3.4), nejsou v současné době v justici údaje ze základních registrů příliš často využívány. Důvodem je zejména skutečnost, že soudy si informace zjišťují z jiných agendových informačních systémů.

Jde především o centrální evidenci obyvatel (dále jen „CEO“), která je agendovým informačním systémem v souladu s ust. § 3 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů. Správcem CEO je Ministerstvo vnitra ČR. Z této agendy soudy a státní zastupitelství čerpají informace o občanech České republiky. Oproti registru obyvatel, který je jedním ze základních registrů, obsahuje CEO podstatně více údajů o osobách. Jde např. o rodná čísla osob, historii trvalých pobytů, údaje o zákazu pobytu, údaje o manželech, partnerech, rodičích, dětech lustrované osoby, o omezení svéprávnosti atd. Tyto údaje soudy a státní zastupitelství při výkonu své činnosti často potřebují. Soudy rovněž do CEO zapisují některé údaje, a to např. rozhodnutí o rozvodu manželství nebo rozhodnutí o neplatnosti či neexistenci manželství a dále rozhodnutí o prohlášení za mrtvého nebo nezvěstného.[46]

[46] Soudům je tato povinnost uložena § 6 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)

Dalším využívaným agendovým informačním systémem je cizinecký informační systém (dále jen „CIS“), jehož správce je v souladu s ust. § 158 zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, Policie České republiky.

Přístup do CEO a do CIS mají soudy zřízen na základě ust. § 175b a 175c zákona o soudech a soudcích. Státní zastupitelství pak podle ust. § 12j zákona č. 283/1993 Sb., o státním zastupitelství. Komunikace s CEO probíhá buď prostřednictvím internetové aplikace po zadání hesla, nebo se dotazy činí přímo z příslušného elektronického systému spisové služby[47] (viz podkapitola 3.9).

Co se týče zjišťování informací o právnických osobách, postačí soudům a státním zastupitelstvím veřejně dostupné evidence, jako jsou veřejné rejstříky či živnostenský rejstřík. I do těchto lze přistupovat prostřednictvím internetové aplikace, nebo se dotazy činí přímo z příslušného elektronického systému spisové služby.

Nevýhodou výše uvedených přístupů je, že zjišťování informací probíhá zásadně na dotaz provedený uživatelem (ať již přes internet či přes elektronický systém spisové služby). U komunikace se základními registry je možné získávat informace jak dotazem uživatele z elektronického systému spisové služby, tak automaticky. Tzn., že při změně referenčního údaje v základním registru se změna promítne automaticky v elektronickém systému spisové služby. Tato možnost však pro technické problémy s tím spojené zatím v justici není funkční.

Soudy a státní zastupitelství, coby orgány činné v trestním řízení, potřebují mít samozřejmě mimo jiné i přístup do rejstříků trestů. I v tomto případě se činí dotazy elektronickou formou přímo z elektronického systému spisové služby a následně se vrací výpisy/opisy ve formátu PDF. Soudy mají rovněž možnost si o výpisy/opisy z rejstříku trestů zažádat prostřednictvím CzechPOINT@Office.

Soudy a státní zastupitelství rovněž mají možnost z elektronických systémů spisové služby lustrovat advokáty v neveřejné části seznamu advokátů spravovaném Českou advokátní komorou. Rovněž funguje automatické upozorňování na např. pozastavení činnosti advokáta či jeho vyškrtnutí ze seznamu.

[47] Organizace justice mají dle ust. § 63 odst. 3 zákona o archivnictví povinnost vést spisovou službu v elektronické podobě v elektronických systémech spisové služby

3.4 Veřejné rejstříky fyzických a právnických osob

Podle ust. § 1 odst. 1 zákona o veřejných rejstřících se s účinností od 1. 1. 2014 veřejným rejstříkem rozumí spolkový rejstřík, nadační rejstřík, rejstřík ústavů, rejstřík společenství vlastníků jednotek, obchodní rejstřík a rejstřík obecně prospěšných společností. Tento nový zákon tak nahrazuje dosud roztříštěnou právní úpravu vedení jednotlivých rejstříků, která byla obsažena v zákoně č. 513/1991 Sb., obchodní zákoník a dále v zákonech č. 227/1997 Sb., o nadacích a nadačních fondech, č. 248/1995 Sb., o obecně prospěšných společnostech, č. 72/1994 Sb. o vlastnictví bytů, č. 83/1990 Sb., o sdružování občanů a č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů. Procesní úprava rejstříkového řízení byla téměř bez změny převzata z o. s. ř. Rejstříky vedené podle těchto zákonů, tedy obchodní rejstřík, nadační rejstřík, rejstřík obecně prospěšných společností a rejstřík společenství vlastníků jednotek, které již před 1. 1. 2014 vedly rejstříkové soudy[48], doplnily nově vzniklý spolkový rejstřík, do kterého se zapisují zejména spolky a odborové organizace a nový rejstřík ústavů. Spolkový rejstřík tvoří z největší části občanská sdružení, která byla do 1. 1. 2014 registrována u Ministerstva vnitra ČR. I tyto nové rejstříky vedou nově rejstříkové soudy. Součástí všech veřejných rejstříků je sbírka listin.

Na veřejné rejstříky lze pohlížet jako na nástroj, který slouží *„k zajištění transparentnosti podnikatelského života.“*[49] S tím úzce souvisí princip materiální a formální publicity. Princip materiální publicity je v souladu se směrnicí Evropského parlamentu a Rady č. 2009/101/ES ze dne 16. září 2009 vymezen v ust. § 8 a násl. zákona o veřejných rejstřících. Nově tedy platí princip materiální publicity pro všechny veřejné rejstříky. Dle tohoto principu se rejstříkový stav zapsaný ve veřejném rejstříku zásadně *„považuje za stav skutečný pro toho, komu není známo, že stav rejstříkový není v souladu se skutečným právním stavem.“*[50] *S* tím souvisí rovněž významný princip formální publicity, podle kterého musí být veřejný rejstřík přístupný každému, kdo má zájem do něj nahlédnout.

Z hlediska eGovernmentu je nutno od sebe odlišovat veřejné rejstříky tak, jak na ně pohlíží zákon o veřejných rejstřících, a které označuje za informační systémy veřejné správy, od elektronických systémů spisových služeb, které slouží ke zpracování návrhů na zápis,

[48] § 1 odst. 4 zákona o veřejných rejstřících
[49] PELIKÁNOVÁ, Irena. *Obchodní právo*. Vyd. 1. Praha: ASPI, 2005. s. 429
[50] PELIKÁNOVÁ, Irena. *Obchodní právo*. Vyd. 1. Praha: ASPI, 2005. s. 444

k vytváření rozhodnutí a následnému přenášení údajů do veřejných rejstříků. Tento vnitřní elektronický (informační) systém rejstříkových soudů, sloužící k evidenci soudních rejstříkových řízení a soudních rejstříků[51], se v současné době označuje jako ISVR (informační systém veřejných rejstříků).

3.4.1 Výpisy z veřejných rejstříků

Podle principu formální publicity, uvedeném v ust. § 3 odst. 1 zákona o veřejných rejstřících, musí soud uveřejnit údaje o zapsané osobě a listiny uložené ve sbírce listin způsobem umožňujícím dálkový přístup a umožnit získat jejich úředně ověřený elektronický opis. Tato ustanovení byla částečně převzata z obchodního zákoníku, ale navíc byla doplněna o jednu podstatnou povinnost, a to umožnit získat úředně ověřený elektronický opis údajů o osobě zapsané ve veřejném rejstříku. Původní obchodní rejstřík byl spuštěn již v roce 1997, přičemž od počátku jde o veřejně přístupnou internetovou aplikaci dostupnou ze stránek www.justice.cz. Od počátku bylo zároveň umožněno bezplatně získávat výpisy (opisy) z obchodního rejstříku a pořizovat si z něj kopie. Šlo však v zásadě o opisy neověřené. Ověřené opisy bylo možné získat pouze na rejstříkovém soudu, později pak přes kontaktní místa Czech POINT. Od 1. 4. 2012 jsou již zveřejňované opisy opatřovány časovým razítkem a označovány uznávanou elektronickou značkou příslušného rejstříkového soudu. Toto lze považovat za výrazný krok v e-Governmentu. Avšak teprve zákon o veřejných rejstřících opisy veřejně přístupné přes internet bezezbytku označil za úředně ověřené. Na takto ověřené opisy lze dle mého názoru dá aplikovat i ust. § 69a odst. 5 zákona o archivnictví, podle kterého „*neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, a následně za doby platnosti uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, nebo uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, opatřen kvalifikovaným časovým razítkem. To platí i pro dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.“* Zákon tak stanoví presumpci pravosti dokumentu v digitální podobě.

[51] viz ust. § 149 a následující instrukce Ministerstva spravedlnosti č. 505/2001-Org, kterou se vydává vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy

Výpisy (opisy) jsou od počátku poskytovány a označovány jako „výpis platných údajů“ (tzv. aktuální výpis) nebo „úplné výpisy“. Ve výpisu platných údajů jsou uvedeny pouze aktuální zapsané skutečnosti, v úplném pak je uvedena i historie jednotlivých zapsaných skutečností. Bohužel v žádném právním předpise nebylo a není stanoveno, v jakém rozsahu může soud opisy poskytovat, co se rozumí částečným a úplným opisem zápisu a zda toto koresponduje se skutečně poskytovanými výpisy. V praxi se objevují i dotazy a námitky veřejnosti, zda musí být skutečně zveřejňovány údaje, které již nejsou platné.

Podle ust. § 4 odst. 1 zákona o veřejných rejstřících rovněž musí soud na žádost vydat „*listinný úředně ověřený částečný nebo úplný opis zápisu nebo listiny uložené ve sbírce listin nebo potvrzení o tom, že určitý údaj ve veřejném rejstříku není, ledaže žadatel výslovně požádá o opis úředně neověřený*.“ Toto ustanovení bylo zcela převzato z obchodního zákoníku a dle mého názoru se jedná o ustanovení z větší části obsolentní. V praxi není možné získat pouze výpis o části zapsaných skutečností (např. jen o zapsaném sídle). Rovněž rozlišování na opisy úředně ověřené a úředně neověřené je zbytečné. V praxi soudy neověřené výpisy poskytovaly naprosto výjimečně, protože byly přístupné přes internet (nyní jsou i tyto již pouze ověřené).

3.4.2 Podání do veřejných rejstříků

Podání ve věcech týkajících se zápisu skutečností do veřejných rejstříků jsou, na rozdíl od jiných soudních řízení, striktně formulářová. V souvislosti s nabytím účinnosti zákona o veřejných rejstřících došlo i ke změně prováděcích předpisů. Vyhlášku č. 414/2011 Sb., o náležitostech formulářů na podávání návrhů na zápis do obchodního rejstříku nahradila nová vyhláška č. 323/2013 Sb., o náležitostech formulářů na podávání návrhů na zápis, změnu nebo výmaz údajů do veřejného rejstříku a o zrušení některých vyhlášek. Tato vyhláška stanovuje náležitosti jednotlivých formulářů. V ust. § 3 odst. 2 pak stanoví povinnost úředně ověřených podpisů na formulářích v listinné podobě. V případě podaní došlých v elektronické podobě (e-mailem, přes tzv. inteligentní formuláře či přes webovou ePodatelnu) musí být formuláře podepsány uznávaným elektronickým podpisem. Nově je zde výslovně stanoveno, že formuláře zaslané z datové schránky osoby, jež návrh na zápis podává, být elektronicky podepsány nemusí. Pokud by však byl formulář zaslán z jiné datové schránky, např. právního zástupce, pak by již nepochybně musela být přiložena elektronicky podepsaná plná moc nebo plná moc, která by byla autorizovaně konvertována.

Způsoby vyplňování formulářů jsou pak nově v souladu s ust. § 22 zákona o veřejných rejstřících stanoveny v nařízení vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob. V ust. § 17 tohoto nařízení je nově uvedeno, že *„pokud zápis, změnu nebo výmaz zápisu ve veřejném rejstříku provádí soud, návrh na zápis, změnu nebo výmaz zápisu se podává prostřednictvím elektronicky vyplněného formuláře na internetových stránkách Ministerstva spravedlnosti. Takto vyplněný formulář lze soudu zaslat jak v elektronické, tak v listinné podobě.“* To neplatí v *„případech, kdy se zápis provádí nebo mění z úřední povinnosti nebo nebyl-li pro zapisované osoby předepsán formulář“*. Dle mého názoru jde v justici o relativně striktní omezení způsobu podávání návrhů, srovnatelné snad pouze s omezením zasílání návrhů na vydání elektronického platebního rozkazu. S účinností od 1. 1. 2014 tak již není možné podávat naprostou většinu návrhů na stávajících formulářích ve formátu ZFO či PDF, ale je nutno využívat pouze tzv. „inteligentní formuláře“, které jsou dostupné na internetových stránkách veřejných rejstříků. Inteligentní formuláře bude možné zaslat elektronicky (po jejich vyplnění se vygeneruje formulář ve formátu PDF) nebo v listinné podobě. Tento krok byl Ministerstvem spravedlnosti zaveden z několika důvodů. V prvé řadě je možno v případě vyplnění inteligentních formulářů zcela využít data v nich obsažená, a automaticky přenést do příslušných usnesení týkajících se zápisu. Dále jsou data využívána k automatické tvorbě záznamů, z nichž následně vznikají opisy z veřejných rejstříků. Soudům tak odpadá pracné přepisování údajů. Dalším důvodem je, že při využití těchto inteligentních formulářů dochází již při jejich vyplňování ke kontrole správnosti některých údajů. Jde zejména o kontrolu adres, zda souhlasí s RUIAN.[52] Rovněž probíhá kontrola, zda jsou vyplněny veškeré náležitosti pro konkrétní právní formu, které se návrh týká.

Přestože od 1. 1. 2014 je možné podávat většinu návrhů pouze na inteligentních formulářích, zejména formuláře pro zápis jsou zasílány soudu téměř výlučně v listinné podobě. Důvodů je několik. Prvním z nich je, že návrh v elektronické podobě musí být v souladu s ust. § 22 odst. 3 zákona o veřejných rejstřících podepsán uznávaným elektronických podpisem nebo zaslán z datové schránky osoby, jež návrh podává. Zejména při tzv. „provozápisu“, tedy zápisu nové osoby do veřejného rejstříku, navrhovatel nedisponuje ani elektronickým podpisem, ani

[52] Zkratka RUIAN se používá pro jeden ze základních registrů, a to registr územní identifikace. Každá adresa v České republice obdrží tzv. RUIAN kód, což je specifický identifikátor dané adresy.

datovou schránkou (ta se mu zřizuje až po jeho vzniku, tedy po zápisu do veřejného rejstříku), proto návrh zasílá v listinné podobně.

Velice často se stává, že návrh na zápis musí podat více osob, např. u veřejné obchodní společnosti všichni společníci, u společnosti s ručením omezeným všichni jednatelé, atd. Na tuto situaci se pak vztahuje ust. § 18 odst. 2 zákona o DS, který v případě nutnosti více podpisů úkonu učiněného datovou schránkou, vylučuje fikci podpisu. Návrh by tak zřejmě museli podepsat elektronickými podpisy všichni navrhovatelé i v případě zaslání datovou schránkou, event. by museli návrh autorizovaně konvertovat.

Dalším problémem jsou přílohy k samotnému návrhu, které jsou ve většině případů originály v listinné podobě a jejich převod do elektronické podoby je při jejich značném množství a ceně autorizované konverze (30 Kč/stranu) finančně nákladný. Dále se k návrhu přikládají přílohy, které musí být rovněž podepsány a často i více osobami zároveň (typicky zakladatelské listiny).

Rovněž není v současné době dořešena problematika placení soudních poplatků. V případě zaslání návrhu na zápis v elektronické podobě informační systém nevyrozumí navrhovatele o platebních údajích (zejména o variabilním symbolu). Navrhovatel proto nemůže zároveň s podáním zaplatit soudní poplatek, ale musí činit dotaz na soud či čekat, až ho soud k zaplacení soudního poplatku vyzve. Placení soudních poplatků platební kartou není v justici možné. Lze tedy konstatovat, že podávání návrhů na zápis čistě v elektronické podobě (někdy označovaný jako on-line zápis) brání velké množství zatím nedořešených problémů.

3.4.3 Podání do Sbírky listin

Co se týče podávání listin do Sbírky listin, i zde došlo k úpravám oproti obchodnímu zákoníku a původní vyhlášce č. 562/2006 Sb. Dle nařízení vlády č. 351/2013 Sb. se listiny, které se zakládají do Sbírky listin, podávají pouze v elektronické podobě ve formátu PDF, což je shodné s předchozí vyhláškou. Nově však není stanoveno, jakým způsobem je možné listiny soudu zasílat. Přicházejí tak v úvahu všechny způsoby elektronické komunikace, které soud akceptuje (tedy datová schránka, e-mail, webová ePodatelna, inteligentní formuláře či technické nosiče dat). Ministerstvem spravedlnosti byly vyvěšeny podrobné informace na

internetových stránkách obchodního rejstříku. Je ovšem otázkou, do jaké míry může soud odmítnout založit do Sbírky listin dokument, který neodpovídá technické specifikaci.

3.4.4 Napojení veřejných rejstříků na ostatní části e-Governmentu

Veřejné rejstříky úzce souvisí rovněž s ostatními částmi e-Governmentu, kterému poskytují důležité informace.

Co se základní registrů týče, tak zde je využívání dat vzájemné. Rejstříkové soudy jsou jedním z hlavních editorů registru osob. Tzn., že veškeré údaje o právnických a fyzických osobách, které jsou zapsány ve veřejných rejstřících, jsou přenášeny do registru osob, ze kterého je poté využívají ostatní orgány státní správy.

Naopak při vedení veřejných rejstříků se využívají údaje jak z registru osob a registru obyvatel, tak i z registru územní identifikace (při zápisu sídla). Pokud rejstříkový soud do veřejných rejstříků zapisuje osobu, která vystupuje např. jako statutární orgán, společník, likvidátor či insolvenční správce, atd., při zápisu využívá údaje uvedené v registru osob či obyvatel. Tyto osoby, jejichž údaje byly převzaty ze základních registrů, jsou pak v pravidelných intervalech aktualizovány. Aktualizace údajů ve veřejných rejstřících vyvolaných změnou v základních registrech je nově upravena i v ust. § 95 odst. 1 zákona o veřejných rejstřících. Toto „párování“ údajů fyzických osob obsažených ve veřejný s údaji v základních registrech má i jeden, pro některé podatele podstatný problém, a tím jsou akademické tituly. Tyto se do registru obyvatel nezapisují, ani zákon o veřejných rejstřících s jejich uváděním nepočítá, nicméně někteří podatelé na jejich zápisu i při aktualizaci údajů trvají. K tomu se již vyjádřil i Vrchní soud v Praze, který ve svém usnesení, č.j. 14 Cmo 114/2013-68, ze dne 25.3.2014 pravil, že *„zápis titulu u fyzické osoby nemůže mít za následek nepřehlednost zápisu v obchodním rejstříku; naopak napomáhá informovanosti třetích osob a může zvyšovat důvěryhodnost společnosti, pokud je ze zápisu v obchodním rejstříku zřejmé, že osoby v něm zapsané mají vysokoškolské vzdělání v oboru, který má společnost zapsaný coby předmět podnikání.“*[53]

[53] Usnesení Vrchního soudu v Praze, č.j. 14 Cmo 114/2013-68, ze dne 25.3.2014

Obdobný princip se využívá i při zápisu tuzemských adres, kde se využívá tzv. „RUIAN kód“, který je přidělen každé budově v České republice. Každé sídlo osoby zapsané ve veřejném rejstříku je tedy spojeno s tímto kódem a v případě změny např. názvu obce či ulice, se tato změna promítne do veřejného rejstříku. I v těchto případech mohou nastat nedomyšlené problémy, a to v případě, kdy bylo obecním úřadem přiděleno číslo popisné, stavebním úřadem vydáno povolení k užívání stavby či kolaudační souhlas, ale stavební úřad dosud nezapsal adresu do RUIAN, zatímco na soud již došel návrh na zápis takového sídla do veřejného rejstříku.

Co se týče propojení s datovými schránkami, tak v souladu s ust. § 5 odst. 1 zákona o DS platí povinnost mít zřízenu datovou schránku pouze pro právnické osoby zřízené zákonem a pro osoby zapsané v obchodním rejstřík a jejich organizační složky. Dle tohoto ustanovení zřídí ministerstvo vnitra ČR datovou schránku bezplatně právnické osobě bezodkladně po jejím vzniku, v případě právnické osoby zapsané v obchodním rejstříku a organizační složky bezodkladně poté, co obdrží informaci o jejím zapsání do obchodního rejstříku. Nelze však v tomto případě spoléhat na podnikatele, že by Ministerstvo vnitra ČR o vzniku právnické osoby sami informovali. Byla tedy zřízena automatická komunikace mezi aplikací ISVR a ISDS. Jakmile je v obchodním rejstříku zapsána nová osoba, aplikací je o tomto automaticky vyrozuměn ISDS, který následně podnikateli datovou schránku zřídí.

Veřejné rejstříky dále automaticky komunikují i s jinými informačními systémy veřejné správy. Jde o tzv. externí odběratele, kteří pomocí veřejných služeb, mimo základní registry, odebírají automatizovaně údaje z veřejných rejstříků. Jde jednak o Czech POINT, prostřednictvím kterého je možné pořizovat výpisy z veřejného rejstříku. Mezi externí odběratele patří i Ministerstvo financí ČR, kterému byla nově v ust. § 7 zákona o veřejných rejstřících stanovena povinnost zveřejňovat dálkovým přístupem údaje o zapsaných osobách v systému administrativního registru ekonomických subjektů (tzv. „ARES“). Účelem je, aby byly veškeré fyzické i právnické osoby, jimž bylo přiděleno IČ, a které jsou vedeny v jakékoliv evidenci, dohledatelné na jednom centrálním místě. Mezi další odběratele patří např. Obchodní věstník, Český statistický úřad, Ministerstvo průmyslu a obchodu ČR (RŽP), Ministerstvo zahraničních věcí ČR, Ministerstvo práce a sociálních věcí ČR, Ministerstvo zemědělství ČR. Způsob této komunikace je upraven vnitřním předpisem, a to instrukcí Ministerstva spravedlnosti č. 26/2000-OI, kterou se stanoví postup pro předávání údajů obchodního rejstříku externím odběratelům.

Dále byla zapracována komunikace mezi aplikacemi pro vedení veřejného a insolvenčního rejstříku. V souladu s ust. § 65 zákona o veřejném rejstříku se do veřejných rejstříků zapisují vybrané údaje o veřejných rejstřících. Protože však nejsou zcela v souladu ustanovení insolvenčního zákona a zákona o veřejných rejstřících (do veřejných rejstříků se zapisuje více údajů o insolvenčním řízení, než má insolvenční soud povinnost soudu rejstříkovému zasílat), byla zapracována vzájemná komunikace mezi oběma rejstříky. Pokud je v insolvenčním rejstříku zveřejněna příslušný dokument o skutečnosti zapisované do veřejného rejstříku (např. zahájení insolvenčního řízení, prohlášení konkursu, atd.), je o tom automaticky okamžitě vyrozuměn rejstříkový soud, který pak posoudí nutnost provedení zápisu do veřejného rejstříku.

3.5 Insolvenční rejstřík

Insolvenční rejstřík je rovněž dle ust. § 419 odst. 1 insolvenčního zákona informačním systémem veřejné správy, jehož správcem je Ministerstvo spravedlnosti ČR. V tomto případě je tedy výslovně uvedeno, že se jedná o ISVS v souladu se zákonem o ISVS, a insolvenční rejstřík se tedy musí řídit pravidly v tomto zákoně stanovenými.

Insolvenční rejstřík lze považovat za velký průlom, co se týče možnosti sledování soudního řízení, kdy se jedná o jediný druh soudního řízení, ve kterém jsou všechny spisy veřejně přístupné, a které lze zcela sledovat prostřednictvím veřejně přístupné internetové stránky. Insolvenční rejstřík obsahuje seznam dlužníků a seznam insolvenčních správců. Jak bylo řečeno v úvodu, jedním z hlavních cílů eGovernmentu je transparentnost činnosti veřejné správy, resp. v daném případě soudní moci. Zveřejněním celého soudního spisu pak došlo dle mého názoru k naplnění tohoto cíle bezezbytku.

Insolvenční rejstřík je internetová aplikace dostupná zcela bezplatně a bez omezení či nutnosti přihlašování. Výjimku z principu publicity tvoří údaje, o kterých tak stanoví zákon. Jde hlavně o ust. § 422 insolvenčního zákona a nově, s účinností od 1.1.2014, ust. § 423 odst. 2 insolvenčního zákona. Podrobnosti jsou pak uvedeny v ust. § 215ga instrukce Ministerstva spravedlnosti ze dne 3. prosince 2001, čj. 505/2001-Org, kterou se vydává vnitřní a

kancelářský řád pro okresní, krajské a vrchní soudy (dále jen v. k. ř.) Soudy tedy musí každý dokument před zveřejněním procházet a kontrolovat, zda neobsahuje citlivé údaje.

V jedné z částí insolvenčního rejstříku, v seznamu správců, je i snadná možnost dohledat, v kolika věcech byl který insolvenční správce určen předsedou soudu. Veřejnost má tak možnost kontrolovat transparentnost při určování správců do jednotlivých řízení.

Za přínos, co se týče větší možnosti veřejné kontroly, lze považovat také tzv. „veřejnou webovou službu“, která umožňuje automaticky sledovat údaje zveřejněné v insolvenčním rejstříku. Ministerstvo spravedlnosti ČR poskytuje webové služby pro sledování insolvenčního rejstříku dvě, a jsou nabízeny zdarma. Na straně uživatelů je však nutno mít nainstalovaný příslušný program, který automatické zpracování údajů umožní. Tyto programy jsou již poskytovány soukromými subjekty, proto bývají zpravidla placené. Cena služby se odvíjí od počtu sledovaných insolvenčních řízení.

3.5.1 Podání v insolvenčním rejstříku

Co se týče způsobu doručování podání do insolvenčního řízení, není ani zde žádná povinnost, a to ani pro insolvenční správce, komunikovat s insolvenčními soudy elektronicky. Podání je tedy možné zasílat jak v elektronické, tak i v listinné podobě. To pak s sebou nese velkou pracnost soudu při zpracování podání. V současné době jsou insolvenční soudy povinny vést soudní spisy duplicitně v listinné a elektronické podobě, což obnáší nemalé finanční, materiální a personální náklady. Podání v elektronické podobě se musí tisknout, podání v listinné podobě pak skenovat a následně zveřejňovat v insolvenčním rejstříku.

Na rozdíl od rejstříkového řízení, není pro většinu podání předepsána zákonem forma formuláře. Insolvenční zákon stanoví povinnost zasílat podání na formulářích pouze u insolvenčního návrhu spojeného s návrhem na povolení oddlužení, u hlasovacích lístků, pro úkon popření přihlášené pohledávky věřitelem a pro přihlášku pohledávky. Všechny tyto formuláře jsou zveřejněny v insolvenčním rejstříku ve formátu PDF.

V současné době je zapracováno automatické přenášení údajů z formuláře pouze pro přihlášky pohledávky. Důvodem je nutnost evidence všech insolvenčních věřitelů, jakožto účastníků insolvenčního řízení, a rovněž vysoký počet došlých přihlášek, kdy denně je soudu

doručeno cca 1000 - 1200 přihlášek pohledávek. Z PDF formuláře přihlášky pohledávky je možné do elektronického systému spisové služby pro vedení insolvenčního řízení (tzv. „ISIR“ – Informační systém insolvenčního rejstříku) přenášet údaje o věřitelích a celkové výši pohledávek. Pokud formulář přijde v listinné podobě, pak se pro přenesení údajů využívají tzv. 2D kódy (QR kódy) umístněné na konci formuláře, s jejichž pomocí lze údaje do aplikace přenést prostřednictvím čteček čárových kódů. Tento způsob využívání informací z podání lze v rámci veřejné správy považovat za výjimečný.

3.5.2 Dokumenty zveřejněné v insolvenčním rejstříku a jejich právní síla

Specifikem insolvenčního rejstříku je, že v souladu s ust. § 71 insolvenčního zákona dochází jeho prostřednictvím i k doručování soudních rozhodnutí účastníkům řízení, zejména věřitelům. Jde tak o doplnění možných doručování podle o. s. ř. S tím úzce souvisí i nutnost zajistit důvěryhodnost zveřejňovaných dokumentů. Dokumenty zveřejňované v insolvenčním rejstříku jsou proto vždy označeny uznávanou elektronickou značkou Ministerstva spravedlnosti ČR a rovněž opatřeny časovým razítkem, což by mělo jejich důvěryhodnost zaručit. Měly by tak být splněny podmínky presumpce pravosti podle již zmíněného ust. § 69a odst. 5 zákona o archivnictví.

V praxi se však přesto vyskytují určité problémy s důvěrou některých orgánů veřejné správy v informace zveřejněné na stránkách insolvenčního rejstříku. Jde zejména o policejní orgány, které trvají na zasílání opisů listinných spisů, či o katastrální pracoviště, která požadují zasílání usnesení týkajících se zpeněžování nemovitostí (např. usnesení o souhlasu soudu s prodejem mimo dražbu) datovou schránkou, přestože jsou veřejně přístupná. Jsem toho názoru, že chybí insolvenčním zákonem přímo stanovená presumpce správnosti údajů zveřejněných v insolvenčním rejstříku, a to nejen pro orgány veřejné moci.

3.5.3 Napojení insolvenčního rejstříku na ostatní části e-Governmentu

Insolvenční soud je jedním z mnoha editorů registru osob, kdy v souladu s ust. § 26 odst. 2 písm. i) zákona o ZR zapisuje do registru osob jeden referenční údaj - právní stav. Jde však pouze o údaj o tom, zda bylo na osobu zahájeno insolvenční řízení, event. konkursní řízení podle již zrušeného zákona o konkursu a vyrovnání. Veškeré podrobnosti o stavu insolvenčního řízení je pak nutno dohledat v insolvenčním rejstříku.

Insolvenční zákon v ust. § 419 odst. 4 rovněž předpokládá možnost vydávat ověřené výstupy z informačního systému veřejné správy o tom, že určitý údaj v insolvenčním rejstříku je nebo není veden. Dle zákona by tak mělo činit Ministerstvo spravedlnosti ČR či soud. V praxi se tak děje zejména prostřednictvím Czech POINTu.

Propojení s aplikací pro vedení veřejných rejstříků již bylo výše zmíněno. Protože však mají některá rozhodnutí vydaná v insolvenčním řízení (např. vyhláška o zahájení insolvenčního řízení, rozhodnutí o úpadku či o prohlášení konkursu) dopad i na průběh jiných soudních řízení, bylo zapracováno automatické přenášení informací i mezi elektronickým systémem spisové služby ISIR a dalšími elektronickými systémy spisové služby. V tomto případě se jedná o komunikaci G2G (government to governemnt), kdy jsou mezi jednotlivými elektronickými systémy soudů přenášeny relevantní informace o průběhu insolvenčního řízení. Na základě těchto automatických podnětů pak soudy rozhodují např. o přerušení řízení v souladu s ust. § 140a či ust. § 263 insolvenčního zákona.

Dále bylo v roce 2013 zapracováno napojení českého insolvenčního rejstříku na připravovaný jednotný evropský insolvenční portál, umožňující vyhledání insolvenčních řízení ve všech veřejně přístupných insolvenčních rejstřících či seznamech dlužníků na základě jednoho dotazu. Ze strany Evropské unie však tento web dosud nasazen nebyl.

V roce 2013 byla Ministerstvem spravedlnosti ČR rovněž vyvinuta aplikace pro možnost sledování insolvenčního rejstříku v mobilním telefonu.

3.6 infoSoud a infoJednání

Jak již bylo výše uvedeno, jedním z cílů eJustice je zajistit transparentní rozhodování soudů a zvýšit informovanost účastníků o průběhu jejich řízení. Na druhou stranu je třeba dbát na ochranu osobních údajů a oprávněných zájmů účastníků řízení. Pro sledování průběhu řízení jsou od roku 2008 provozovány aplikace infoSoud a infoJednání, ve kterých se zobrazují ty nejzákladnější údaje o soudním řízení, resp. o nařízených soudních jednáních. Jde o úzce propojené internetové aplikace dostupné z internetových stránek www.justice.cz. V obou aplikacích je možno vyhledávat řízení zásadně podle jejich spisové značky. Nejsou zde

zveřejňovány žádné údaje o účastnících řízení, ani žádné dokumenty obsažené v soudním spisu. Aplikace infoSoud slouží zejména ke sledování průběhu řízení. Jde především o údaje o podání návrhu na zahájení řízení, údaje o rozhodování ve věci samé a o podání opravného prostředku, řádného i mimořádného. V roce 2012 byla aplikace infoSoud rozšířena i o možnost vyhledávání údajů o odvolacím či dovolacím řízení. Zobrazují se zde tedy řízení vedená u okresních, krajských, vrchních soudů a u Nejvyššího soudu ČR. Tato aplikace je výhodná pro účastníky řízení v tom, že si jejím prostřednictvím dokáží zjistit informace např. o rozhodnutí ve věci či o podání opravného prostředku dříve, než jim jsou doručeny soudem. Další výhodou je možnost zjistit si přes internet spisové značky odvolacího či dovolacího soudu, aniž by bylo nutno činit dotaz na soud. Ostatní veřejnost může sledovat průběh řízení pouze v případě, kdy zná spisovou značku, pod kterou je řízení u konkrétního soudu vedeno. Aplikace infoJednání pak slouží k přehledu o nařízených jednáních ve věci. Jsou zde i informace o místě a času konání jednání. Tyto informace jsou však pouze doplňující, aplikace v žádném případě nenahrazuje povinnost soudů doručovat účastníkům předvolání k jednání.

Nevýhodu obou aplikací vidím zejména v tom, že v současné době neexistuje jejich legislativní zakotvení, které by dodávalo poskytovaným informacím jakoukoliv právní relevanci. Jde tedy nyní pouze o doplněk informací, které musí soudy účastníků řízení přesto zasílat v elektronické či listinné podobě.

3.7 infoData a Judikatura

V roce 2010 byla Ministerstvem spravedlnosti ČR spuštěna internetová aplikace infoData, dostupná rovněž ze stránek www.justice.cz. Aplikace obsahuje výkazy o činnosti soudů a státních zastupitelství, přehledy statistických listů soudů a státních zastupitelství a rovněž statistické ročenky. Jde o poskytování statistických informací zveřejněním (tedy aktivně) v souladu s ust. § 4 zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Zatímco výkazy slouží k informování o činnosti soudů a státních zastupitelství (tzn., např. kolik bylo podáno žalob, jak o nich bylo rozhodnuto a v jakém čase, atd.) v určitém časovém úseku, statistické listy informují o pravomocně skončených řízeních a daleko podrobněji vypovídají o charakteru nápadu a o rozhodnutích ve věci. Výkaznictví a statistika je v justici velice podrobná, existuje 63 výkazů pro jednotlivé soudní agendy a 5 druhů statistických listů. Zpracování výkazů a statických listů je upraveno v instrukci Ministerstva spravedlnosti č.

68/2011-OD-ST, o statistickém sledování v resortu justice – agendy soudů a v instrukci č. 69/2011-OD-ST, o vnitřním informačním systému resortu justice - agendy státních zastupitelství. Jednotlivé údaje do výkazů se přenáší automaticky na základě údajů vytvořených v jednotlivých elektronických systémech spisové služby a následně přenesených do aplikace CSLAV DW[54]. Statistické listy vyplňují zaměstnanci soudů v příslušných elektronických systémech spisové služby a údaje se z nich opět přenáší a následně sčítají v aplikaci CSLAV DW.

Zprovoznění této aplikace lze dle mého názoru považovat za velký krok k informování odborné i laické veřejnosti o rychlosti a způsobu rozhodování v jednotlivých soudních agendách. Veřejnost má možnost porovnávat rychlost a způsob rozhodování na jednotlivých soudech a tyto údaje používat pro další účely (např. psaní kvalifikačních prací, odborných článků, apod.)

Další aplikací provozovanou Ministerstvem spravedlnosti ČR sloužící k informování veřejnosti o rozhodování soudů, ale i o tom, jak soudy vykládají právo či jednotlivá ustanovení zákonů, je internetová aplikace Judikatura, dostupná ze stránek www.justice.cz. V ní soudy zveřejňují anonymizovaná rozhodnutí krajských a vrchních soudů, která byla příslušným evidenčním senátem určena jako významná a následně zařazena do jedné ze skupin judikátů. Postup soudů při evidenci judikatury je upraven v instrukci Ministerstva spravedlnosti ČR, č. j. 20/2002 SM, kterou se upravuje postup při evidenci a zařazování rozhodnutí okresních, krajských a vrchních soudů do systému elektronické evidence soudní judikatury. Povinnost zveřejňovat judikáty na internetu je stanovena od 1. 3. 2011.

3.8 infoDeska

Internetová aplikace infoDeska slouží zejména ke zveřejňování písemností dle ust. § 50l odst. 3 o. s. ř. Každý soud má tedy povinnost zveřejňovat písemnosti jak na své „dřevěné" úřední desce, která se nachází většinou na chodbě soudu, tak souběžně i způsobem umožňujícím dálkový přístup, což se děje právě přes tzv. „elektronickou úřední desku“ čili infoDesku. Na úřední desce se dále zveřejňují povinné informace ust. dle § 5 zákona č. 106/1999 Sb. či

[54] V aplikaci CSLAV DW se shromažďují a zpracovávají data z jednotlivých výkazů a statistických listů

vyhlášky č. 259/2012 Sb. Postup zveřejňování je upraven v instrukci Ministerstva spravedlnosti č. 157/2008-OD-ST, kterou se upravují povinnosti a postup při zveřejňování informací v aplikaci infoDeska resortu justice.

Za velký nedostatek považuji nutnost souběžného zveřejňování listin, zejména těch podle ust. § 50l o. s. ř., jak na úřední desce soudu, tak v aplikaci infoDeska. Jsem toho názoru, že by mělo být o. s. ř. stanoveno, že postačuje listiny zveřejnit na elektronické úřední desce. Podstatným způsobem by to usnadnilo práci soudním kancelářím. Další možností je nahradit „dřevěnou“ úřední desku interaktivními panely či obrazovkami.

3.9 Spisová služba a elektronické spisy v justici

Jak již bylo uvedeno, vedení spisové služby v elektronické podobě lze považovat za jednu z nejdůležitějších části eGovernentu, tedy i eJustice. Soudy a státní zastupitelství, jakožto organizační složky státu, mají podle ust. § 63 zákona o archivnictví povinnost vést spisovou službu v elektronické podobě, není-li zákonem stanoveno jinak. Spisová služba je ve všech organizacích justice vedena v elektronických systémech spisové služby.

Spisové služby v justici můžeme dělit podle různých kritérií např.:

Podle toho, zda slouží k vedení elektronických spisů či nikoli

Jak již bylo uvedeno, spisová služba v elektronické podobě neznamená, že i spisy jsou vedeny v elektronické podobě. Možnost vedení elektronických soudních spisů není dána zákonem o archivnictví, ale ust. § 40b o. s. ř. a následně podrobně upravena v jednacím řádu a ve v. k. ř. U elektronického spisu jsou veškerá rozhodnutí vyhotovena v elektronické podobě a následně podepsána v elektronické podobě. Dokumenty došlé od účastníků řízení a dalších osob v listinné podobě se skenováním převádí do elektronické podoby a soud tak pracuje a účastníci nahlíží pouze do elektronického spisu. Mimo spisů v rejstříku EPR, do kterého se zapisují návrhy na vydání elektronického platebního rozkazu podle ust. § 174a o. s. ř., se všechny ostatní spisy v justici vedou primárně v listinné podobě.

Spisové služby procesně orientované či evidenčně orientované

Procesně orientovanou spisovou službou se rozumí taková, která nejen slouží k evidenci jednotlivých spisů a dokumentů, ale zároveň vede uživatele k tomu, jak ve věci postupovat a aktivně mu pomáhá jak s vyhotovením rozhodnutí a jeho rozesláním, tak i s většinou dalších kroků ve spisu. V justici jde však vzhledem k zásadě nezávislosti soudů a složitosti soudního procesu o funkčnost spisové služby nanejvýš spornou, protože uživatele podstatným způsobem omezuje v úkonech, které je možno ve spisu vykonat. V současnosti lze za procesně orientované spisové služby považovat CEPR[55] a ISVR.

Centralizované či decentralizované

Jde o technické uspořádání a architekturu elektronických systémů spisové služby, které ovšem mají procesní důsledky např. v jednotném přidělování spisové značky přes všechny soudy či možnosti nahlížení do spisů jiných soudů, státních zastupitelství, atd.

Stejně jako je eJustice specifická část eGovernmentu, tak i elektronické systémy spisové služby používané v justici mají řadu specifických funkcí.

Obecně všechny spisové služby slouží k evidenci soudních rejstříků (například rejstřík C pro civilní řízení, rejstřík T pro trestní věci, rejstřík EXE pro exekuční řízení, atd.) a v nich evidovaných spisů označených spisovými značkami v souladu s v. k. ř. Vyznačují se v nich pohyby spisů (např. zda se spis nachází u soudce, vyššího soudního úředníka, zapisovatelky, atd.). Dále se v nich vede evidence jednotlivých dokumentů obsažených ve spise (ve smyslu spisového přehledu). Eviduje se vyřízení jednotlivých spisů (způsob vyřízení, právní moc, podání opravného prostředku, odeslání nadřízenému soudu, atd.). Mohou se v nich vytvářet rozhodnutí a přípisy či jiné písemnosti. V každém systému se evidují účastníci řízení a další osoby (tzv. „seznam jmen“[56]), které jsou pak propojeny s jednotlivými spisovými značkami. Tyto údaje se následně využívají např. při lustraci účastníků řízení, či při odesílání písemností. Spisové služby umožňují odesílat dokumenty do datové schránky účastníků a jiných osob. Dále se jejich prostřednictvím odesílají dokumenty na elektronickou úřední desku a informace do aplikací infoSoud a infoJednání. Ve většině případů se prostřednictvím spisových služeb rozdělují spisy k vyřízení mezi jednotlivé soudní senáty. V neposlední řadě

[55] CEPR – centrální elektronický platební rozkaz je první elektronický systém spisové služby, který umožňuje vést soudní spisy v čistě elektronické podobě (viz dále)

[56] Seznam jmen je jmenný rejstřík ve smyslu ust. § 25 vyhlášky č. 259/2012 Sb. do kterého se zapisují zejména účastníci řízení, al i jiné osoby, která v řízení vystupují (svědci atd.)

se jejich prostřednictvím shromažďují a odesílají data pro výkazy a statistiky do aplikace CSLAV.

Bohužel postupným vývojem došlo k tomu, že se v justici používá několik elektronických systémů spisových služeb od několika dodavatelských firem. V současné době se v justici používají tyto elektronické systémy spisových služeb:

ISAS – Informační systém administrativy soudů. Jedná se o nejstarší informační systém využívaný v justici od roku 1997. Vedou se v něm všechny soudní rejstříky okresních soudů (tedy civilní, trestní, exekuční, výkon rozhodnutí, opatrovnický, rejstřík nejasných podání, atd.) s výjimkou rejstříku EPR, který se vede v aplikaci CEPR. Jde o systém evidenčně orientovaný a decentralizovaný. Kromě všech výše uvedených obecných funkcí obsahuje rovněž automatický systém přidělování obhájců podle ust. § 39 trestního řádu. Rovněž obsahuje správní deník, modul knihovna atd., které používá správa soudu pro svoji činnost.

CEPR – Centrální elektronický platební rozkaz. Je naopak nejmladším a nejmodernějším informačním systémem v justici. Nasazován byl postupně od roku 2012 na okresní a krajské soudy. Jde o systém procesně orientovaný, centrální a jako jediný v justici určený pro vedení elektronických spisů. Jde o první a zatím jedinou aplikaci, která nahradila dosavadní listinné spisy, což umožnilo ust. §40b odst. 1 o. s. ř. Tuto aplikaci lze také považovat za výchozí pro další rozšiřování elektronických spisů v justici. Do CEPRu se zapisují návrhy na vydání elektronického platebního rozkazu podle ust. § 174a o. s. ř., které jsou vyplňovány v PDF formuláři. Po jejich podepsání elektronickým podpisem a odesláním do centrální podatelny se data z formuláře přenesou do CEPRu. Následně v aplikaci proběhnou zcela automaticky rutinní úkony (lustrace účastníků proti CEO, veřejným rejstříkům, atd.) a referentovi je předpřipraveno rozhodnutí, tedy elektronický platební rozkaz či jiné procesní rozhodnutí. To je následně podepsáno elektronickým podpisem osoby, která jej vydala, a rozesláno účastníkům řízení. Jde rovněž o první aplikaci, která při odesílání rozhodnutí či jiných písemností využívá tzv. hybridní poštu. Tzn., že soud netiskne klasické „zelené“ obálky, ale do střediska provozovatele systému hybridní pošty (což je nyní Česká pošta, s. p.) je odeslán PDF dokument s rozhodnutím, který je následně zcela automaticky vytištěn a vložen do vyplněné obálky přímo na pracovišti provozovatele systému hybridní pošty. „*Právní základ tohoto doručování ministerstvo vložilo do § 48 odst. 4 OSŘ, podle nějž doručuje-li se prostřednictvím provozovatele poštovních služeb, stejnopisy rozhodnutí a jiné písemnosti*

soudu v listinné podobě mohou být vyhotovovány za součinnosti tohoto provozovatele; podrobnosti takového postupu stanoví prováděcí právní předpis. Tím je jednací řád pro okresní a krajské soudy, který byl pro tyto účely novelizován vyhláškou č. 438/2011 Sb.[57] Nespornou výhodou vedení elektronického spisu je uživatelský komfort jak pracovníků soudů, tak i účastníků řízení, dále snížení finančních nákladů na kancelářské potřeby a v neposlední řadě i bezpečnost systému. Příslušnému referentovi je předpřipraveno rozhodnutí, čímž je ušetřen čas na jeho přípravu. Dále nemusí kancelář soudu činit úkony spojené s doručováním účastníkům, většinu práce zastane sama aplikace (vyhledávání DS a případně odesílání PDF hybridní poště). Spis je přístupný referentovi 24 hodin denně odkudkoliv. Další výhodou je bezpečnost. „*Elektronický soudní spis existuje paralelně na dvou fyzicky oddělených serverech a zálohován je ještě na třetím fyzicky i technologicky odděleném zařízení (v datové knihovně).*“[58]

ISKS – Informační systém krajských soudů. Jde o systém evidenčně orientovaný a decentralizovaný. Evidují se v něm spisy konkursní a vyrovnací podle zákona č. 328/1991 Sb., o konkursu a vyrovnání (rejstříky K a KV). Dále se do něj tzv. „převádí“ spisy, ve kterých byl krajským soudům podán návrh na vydání elektronického platebního rozkazu, ale elektronický platební rozkaz vydán z různých důvodů nebyl, nebo byl po podání odporu zrušen.

ISVKS – Informační systém vrchních a krajských soudů. Jde o systém evidenčně orientovaný a decentralizovaný. Nahradil v roce 2001 systém ISKOS. Je v něm vedena většina rejstříků (jak provostupňových, tak i odvolacích a správy soudu) používaných na krajských a vrchních soudech (např. rejstříky Cm, Co, To, T, C, atd.).

ISIR – Informační systém insolvenčního rejstříku. Byl nasazen na krajské a vrchní soudy a na Nejvyšší soud v roce 2008, spolu s účinností insolvenčního zákona a vedou se v něm rejstříky INS (insolvenční řízení) a ICm (incidenční spory). Kromě obecných funkcí slouží zejména ke zveřejňování dokumentů v insolvenčním rejstříku. Dále v něm probíhá určování insolvenčních správců v souladu s ust. § 25 insolvenčního zákona. Stejně jako v CEPRu se v něm evidují v elektronické podobě všechny dokumenty obsažné ve spise, ale s tím rozdílem,

[57] KORBEL, Fratišek. Elektronická spravedlnost (2). *Právo & Byznys*. 2012, 1/2012, str. 25
[58] KORBEL, Fratišek. Elektronická spravedlnost (2). *Právo & Byznys*. 2012, 1/2012, str. 25

že se souběžně vede i listinný spis, který je primární. Nelze tedy mluvit o elektronickém soudním spisu, a to i s ohledem na ust. § 21 jednacího řádu, který stanoví, že *„rozhodnutí se vyhotovují v té podobě, v jaké je veden spis.“* V insolvenčním řízení jsou originály rozhodnutí tvořeny v listinné podobě. Jde o systém centrální a evidenční.

ISVR – Informační systém veřejného rejstříku. Byl nasazen na krajské soudy v roce 2012. Slouží k vedení rejstříku F, kam se zapisují návrhy týkající se veřejných rejstříků (spolkový rejstřík, nadační rejstřík, rejstřík ústavů, rejstřík společenství vlastníků jednotek, obchodní rejstřík a rejstřík obecně prospěšných společností). Jde o centrální a procesně orientovaný systém. Tvoří se v něm veškerá rozhodnutí a jeho prostřednictvím se ve veřejných rejstřících poskytují výpisy.

ISNS – Informační systém Nejvyššího soudu. Slouží pouze k vedení rejstříků Nejvyššího soudu ČR. Jde prakticky o upravenou verzi informačního systému ISAS upravenou pro potřeby Nejvyššího soudu ČR. Jde o systém evidenčně orientovaný a decentralizovaný

ISNSS - Informační systém Nejvyššího správního soudu. Slouží pouze k vedení rejstříků Nejvyššího správního soudu ČR. Na rozdíl od ostatních aplikací si správu tohoto informačního systému zajišťuje Nejvyšší správní soud samostatně. Jde o systém evidenčně orientovaný a decentralizovaný

ISYZ – Informační systém státních zastupitelství. Slouží ke komplexnímu vedení rejstříků všech stupňů státních zastupitelství. Jde o obdobu ISASu upravenou pro potřeby státních zastupitelství.

IRES – Informační systém pro vedení ekonomických agend. Je nasazen na všech stupních soudů a státních zastupitelství a slouží pro ucelené zpracování ekonomických a účetních dokladů. Evidují se v něm soudní poplatky a jejich vymáhání, faktury, smlouvy, majetek, rozpočet, pokladna, banky, pohledávky a závazky atd. Je propojen se státní pokladnou.

AIS PMS - Administrativní informační systému Probační a mediační služby. Jde o systém evidenčně orientovaný a decentralizovaný.

Jednotlivé elektronické systémy spisové služby jsou sice od sebe odděleny, z procesních důvodů a pro usnadnění práce soudů a státních zastupitelství však existuje mezi nimi značné množství vzájemných komunikací, jako např.:

- propojení ISAS – ISYZ pro předávání dat o podaných obžalobách a návrzích na potrestání a následné předávání dat zpět o způsobu rozhodnutí v trestních věcech,
- propojení ISAS – ISVKS pro předávání dat o podaných opravných prostředcích a následně zpět o způsobu jejich vyřízení,
- propojení ISAS (ISKS, ISVKS, ISNS) – ISIR pro předávání dat o zahájených insolvenčních řízeních, o prohlášení úpadku a konkursu a jejich skončení,
- propojení aplikací ISAS – CEPR pro přenos dat ve věcech, ve kterých byl podán odpor proti elektronickému platebnímu rozkazu, a tyto byly následně převedeny do rejstříku C,
- propojení ISIR – ISVR pro předávání dat o zahájených insolvenčních řízeních a dalších informací v souladu s ust. § 65 zákona o veřejných rejstřících,
- propojení ISAS, ISIR, CEPR, ISKS, ISVKS – IRES – pro předávání informací o předepsaných soudních poplatcích, atd.

a další propojení mezi elektronickými systémy spisové služby, které se v čase vyvíjí a rozšiřují.

Předmětem časté kritiky elektronických systémů spisové služby v justici je však nejen jejich vzájemná nekompatibilita, ale i malá uživatelská přívětivost.

3.10 Elektronické dokumenty a dokazování v soudním řízení

Listiny jsou v souladu s ust. § 125 o. s. ř. jedním z důkazních prostředků v soudním řízení. Elektronický dokument se tak může stát důkazním prostředkem. Výhodou elektronického dokumentu z tohoto pohledu je, že způsobem svého vzniku (tedy zvýšenou precizností při elektronizaci) mohou poskytovat vyšší důvěru než dokumenty v listinné podobě. Pravostí dokumentů se zabývá více právních předpisů. Je jím zákon o archivnictví, ve svém již zmíněném ust. § 69a odst. 5.

Obdobné ustanovení bylo i přidáno do zákona o elektronickém podpisu novelou č. 440/2004 Sb. a ust. § 11 odst. 2 tak stanovilo, že „*písemnosti orgánů veřejné moci v elektronické podobě označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány*." Tímto ustanovením, které však bylo zrušeno novelou účinnou od 1. 7. 2012, tak byla zakotvena veřejná elektronická listina.

Dalším ustanovením upravujícím elektronické dokumenty v soudním řízení je ust. § 134 o. s. ř., podle kterého „*listiny vydané soudy České republiky nebo jinými státními orgány v mezích jejich pravomoci, jakož i listiny, které jsou zvláštními předpisy prohlášeny za veřejné, potvrzují, že jde o nařízení nebo prohlášení orgánu, který listinu vydal, a není-li dokázán opak, i pravdivost toho, co je v nich osvědčeno nebo potvrzeno.*"

Rozdíl mezi veřejnými a soukromými listinami tedy spočívá v tom, že „*u veřejných je třeba, aby to prokázal ten, kdo jejich pravost popírá (ust. §134 o. s. ř), kdežto u soukromých musí v případě zpochybnění naopak její pravost a obsah dokazovat ten, kdo se jich dovolává.*"[59]

Jak však dle mého názoru někteří autoři správně uvádí, „*dokument nelze brát ani jako totální či a priori spolehlivý důkaz. Důkazní spolehlivost může být i u elektronického dokumentu konstatována až jako výsledná kombinace jednotlivých skutkových informací. Z hlediska fungování elektronického dokumentu v roli důkazního prostředku, tak není velkého rozdílu od možností dokumentů listinných. Elektronický dokument je tedy stejně dobrým důkazním prostředkem jako listinný dokument a jeho důkazní hodnota závisí na dalších okolnostech nikoliv na formě.*"[60]

3.11 Další projekty e-Justice

Mimo uvedené hlavní části eGovernemtu bylo vytvořeno, nebo se aktuálně vytváří, množství dalších elektronických aplikací, které mají organizacím justice, účastníkům řízení i široké veřejnosti pomoci při každodenní činnosti.

[59] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2. vydání. Leges, 2012. s 253
[60] LECHNER, Tomáš. *Elektronické dokumenty v právní praxi /: Tomáš Lechner*. Praha: Leges, 2013, s. 193

Jednotlivé soudy a státní zastupitelství mají povinně zřízeny internetové stránky, na kterých poskytují základní informace pro účastníky řízení. Např. kontaktní informace, informace o příjmu elektronických podání, o rozvrhu práce, jejich prostřednictvím je možné prohlížet elektronickou úřední desku atd. Ministerstvo spravedlnosti poskytuje na svých internetových stránkách přístupy do ze zákona vedených rejstříků (veřejné rejstříky, insolvenční rejstřík, evidence úpadců), dále do povinně vedených seznamů (seznam rozhodců, seznam mediátorů, seznam znalců a tlumočníků, registr poskytovatelů pomoci obětem trestných činů). Nad rámec zákona však poskytuje i informace o právu pro širokou veřejnost (např. internetové stránky nového občanského zákoníku či insolvenčního zákona).

Jednou z aplikací využívanou soudy, státními zastupitelstvími a Probační a mediační službou je Centrální evidence stíhaných osob (CESO). Podle ust. § 12i zákona č. 283/1993 Sb., o státním zastupitelství je státní zastupitelství pro potřeby orgánů činných v trestním řízení a Probační a mediační služby „*oprávněno vést centrální evidenci stíhaných osob, která obsahuje osobní údaje vztahující se k osobám, proti kterým se trestní řízení vede, k poškozeným, popřípadě k dalším osobám na trestním řízení zúčastněným a dále údaje k trestným činům, které byly nebo měly být spáchány, a údaje s tím bezprostředně související. Informace z centrální evidence stíhaných osob lze použít pouze pro účely trestního řízení*“. Dále zákon umožňuje přístup do CESO také národnímu členu Eurojustu a za určitých podmínek na vyžádání též Ministerstvu spravedlnosti.

S účinností od 1. 1. 2013 byl na základě novely zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád), zřízen ust. § 35b rejstřík zahájených exekucí (dále jen „RZE“). Podle zákona jde o elektronický seznam, který zřizuje a spravuje Ministerstvo spravedlnosti. Jde o seznam neveřejný, do něhož mají přístup pouze soudy a exekutorská komora. Údaje do něj podle exekučního zákona zapisují soudy a jednotliví exekutoři. V praxi je zápis ze strany soudů zcela automatizován. Pokud soudu dojde od exekutora návrh na pověření a nařízení exekuce podle ust. § 43a odst. 1 exekučního řádu, který musí být na předepsaném formuláři (tzv. „EŽOPEX“), a který se zasílá určeným způsobem, tak se údaje po doručení na centrální podatelnu soudů automaticky zapíší do RZE, zcela bez zásahu soudu. Po technické stránce je RZE internetová aplikace. Okresní soudy do ní mohou nahlížet přes aplikaci ISAS, krajské soudy a exekutoři pak využívají internetový

prohlížeč. Exekutoři do ní mohou zapisovat zákonem stanovené údaje ručně nebo pomocí webových služeb prostřednictvím svých spisových služeb.

V současné době se připravuje možnost usnadnění podávání žalob o drobných nárocích v souladu s nařízením Evropského parlamentu a Rady č. 861/2007 ze dne 11. července 2007, kterým se zavádí evropské řízení o drobných nárocích. Hlavním účelem úpravy je umožnit přijímat standardizované formuláře a ověřovat u nich elektronické podpisy na základě tzv. „Circle of Trust“, kdy přijímající strana (soud v České republice) nepotřebuje ověřovat platnost podání, podpisů a certifikátů a může spoléhat pouze na informace uvedené v tzv. Tokenu, což je PDF soubor připojený k podání.

Dále se připravuje elektronická komunikace s Českou správou sociálního zabezpečení ve věcech předávání údajů o vyplacených dávkách nemocenského a důchodového pojištění.

Rovněž se připravuje a testuje projekt tzv. videokonferencí, prostřednictvím kterých by se měly snížit výdaje na výslechy vazebně stíhaných osob. Jde zejména o úspory za eskorty stíhaných osob a do budoucna i úspory za cestovné svědků.

3.12 Shrnutí kapitoly

Cílem této kapitoly bylo ukázat velice blízké propojení e-Governmentu a eJustice, která téměř veškeré jeho základní části bezezbytku využívá (elektronické podpisy, datové schránky, atd.). Nadto však eJustice zavedla množství dalších prvků, které mohou účastníci řízení a široká veřejnost při uplatňování jejich ústavního práva na soudní ochranu využívat. Smyslem bylo poukázat, jak teoretické koncepty eGovernmentu popsané v různé odborné literatuře fungují či nefungují ve skutečnosti.

4. Porovnání teoretického vymezení eGovernmentu a reálné praxe ukázané na příkladu eJustice

Cílem eGovernmentu, jak již bylo uvedeno, je poskytovat lepší služby veřejnosti a občanům prostřednictvím informačních technologií a umožnit jim podílet se na správě věcí veřejných a tím posílit demokratizaci veřejné správy. V České republice se však rozvoj elektronizace veřejné správy dosud omezil zejména na elektronickou komunikaci s orgány veřejné moci a stejně tak na výměnu a sdílení elektronických dat o osobách. Možnosti e-participace občanů jsou v současné době značně omezené.

O skutečném eGovernmentu můžeme v České republice hovořit až od nabytí účinnosti zákona o elektronickém podpisu, tedy od roku 2001. Jde tedy relativně o mladou problematiku, která se vyvíjí rychlým tempem, a u které probíhá neustálý boj mezi pokrokem techniky a nároky společnosti na řádnou správu na straně jedné, a na pomalu a těžce vznikající legislativu a pomalost státních orgánů na straně druhé.

To vše je ztíženo nekoncepčností a překotností rozvoje eGovernemtu a jeho legislativní úpravy. Přestože hlavní institucí, která by měla zastřešovat celý rozvoj, je dle současné legislativy Ministerstvo vnitra ČR, a přestože v jeho působnosti vznikají všechny hlavní právní normy upravující eGovernment, dochází k nejasnému a protichůdnému vymezení základních pojmů. Praxe je taková, že je schválena norma a teprve následně se zjišťuje, jaké bude mít následky v praxi. Pro oblast justice je třeba důsledně pamatovat a domýšlet, jaký mohou mít změny legislativy v oblasti eGovernmentu dopad na ústavní právo na soudní ochranu, zejména zda neznemožní občanům přístup ke spravedlnosti.

4.1 Zhodnocení využívání jednotlivých částí eGovernmentu v justici

Jsem toho názoru, že i přes všechny popsané problémy spojené se zaváděním eGovernmentu v justici lze konstatovat, že využívání jeho jednotlivých částí je funkční.

Orgány justice, zejména soudy a státní zastupitelství, přijímají podání v elektronické podobě zcela v souladu s ust. 64 odst. 1 zákona o archivnictví a vyhláškou č. 259/2012. Tato komunikace se stala pro velkou část účastníků soudního řízení standardním způsobem zasílání

podání organizacím justice a počet elektronických podání neustále roste. Vnitřní organizace příjmu podání byla ze strany Ministerstva spravedlnosti upravena instrukcí č. 133/2012-OD-ST. Troufám si říci, že co do vstřícnosti k veřejnosti šla justice nad rámec povinností daných zákonem, kdy přijímá kromě e-mailů a datových zpráv z datových schránek i další typy datových zpráv a nad rámec zákona o archivnictví přijímá i některé časté typy datových formátů dokumentů. Dále nad rámec vyhlášky podrobně informuje podatele o příjmu a výsledku ověřování jeho elektronických podpisů.

I přes počáteční problémy při zavádění datových schránek obecně, včetně justice, se domnívám, že v roce 2014 lze již hovořit o stabilním systému, který ušetřil v justici značné finanční náklady spojené s doručováním a také zrychlil soudní proces, zejména u sporů, kde jedním z účastníků je právnická osoba. K datovým schránkám v justici již byla vytvořena dostatečná judikatura, o kterou je možno se opřít. Za další krok správným směrem považuji již zmíněnou novelizaci procesních ustanovení v justici, které aktuálně jasně stanoví, že není nutné v případě podání zaslaného datovou schránkou opatřovat toto podání elektronickým podpisem.

Co se týče základních registrů, komunikace s nimi je v plné míře využívána v případě vedení veřejných rejstříků fyzických a právnických osob rejstříkovými soudy, kde jsou rejstříkové soudy jak editory referenčních údajů v registru osob, tak i jejich velkými uživateli. Rovněž insolvenční rejstřík plní svoji zákonnou úlohu editora registru osob. V ostatních soudních agendách zatím údaje ze základních registrů příliš využívány nejsou a místo nich se používají stávající evidence (jako CEO či registr cizinců, atd.). Rovněž není funkční automatické využívání údajů ze základních registrů, a to zejména pro svoji technickou náročnost.

Prostřednictvím služeb Czech POINT je možno získávat výpisy z veřejných rejstříků a z insolvenčního rejstříku, čímž se usnadnila jejich dostupnost pro širokou veřejnost.

Veškerá spisová služba je v justici vykonávána v elektronické podobě v elektronických systémech spisové služby v souladu s ust. § 63 odst. 3 zákona o archivnictví. Značným problémem je nekompatibilita jednotlivých systémů. Spisové služby ISAS, ISKS, ISIR, IRES, CEPR, ISYZ, ISNS jsou dodávány firmou CCA Group, a.s., a založeny na technologii Oracle. Spisovou službu ISVKS dodává firma VUMS Legend, s.r.o., a je založena na platformě IBM, Lotus Notes. ISVR pak dodává firma Corpus Solutions, a.s., a jde o webovou aplikaci. Dle

mého názoru není nutné, a ani žádoucí, aby veškeré informační systémy v justici dodávala jedna společnost, ale všechny informační systémy by měly být založeny na stejné platformě a vzájemně kompatibilní a propojené, což nyní zdaleka nejsou.

Nad rámec zákonných povinností orgány justice, resp. Ministerstvo spravedlnosti ČR zavedlo a zavádí další prvky eGovernmentu. Jde o zmíněné aplikace z „rodiny info" jako je infoSoud, infoJednání, infoData, eJudikatura, ale i elektronické soudní spisy, veřejná webová služba insolvenčního rejstříku, atd.

4.2 Rizika spojená s rozvojem eGovermentu pro oblast justice

Stejně jako u eGovernmentu, i při budování eJustice chybí základní koncepce toho, čeho se chce při elektronizace justice dosáhnout. Každý orgán veřejné správy má svá specifika a své činnosti vyplývající z jeho poslání stanoveného právními předpisy. V justici je vše ještě umocněno ústavními principy nezávislostí jak soudů, tak i soudců. Informační systémy a jejich rozvoj je však v působnosti Ministerstva spravedlnosti ČR, proto jakýkoliv rozvoj a další postup elektronizace je vždy „balancování na hraně". Základní otázka pro další elektronizaci justice zní: Lze vůbec soudy či soudce přinutit při práci využívat počítač a informační technologie? A na to navazují další otázky.

Existují různé názory na hlavní směr elektronizace justice. „*Je třeba zdůraznit, že centrálním institutem justice z informační perspektivy není podání, rozhodnutí nebo lhůta, ale spis. Jakákoli koncepce elektronické justice tedy musí být nutně postavena na jednotícím základě elektronického spisu a jeho zabezpečení.*"[61]

Ale co když soudce odmítne pracovat s elektronickým spisem? Jde o zásah do nezávislosti soudů či nikoliv? A pokud lze soudy a soudce „donutit" pracovat s počítačem, jak moc může elektronický systém spisové služby omezovat uživatele v jeho práci s tímto spisem?

Toto „balancování na hraně" se plně projevuje v případě aplikací CEPR a ISVR, což jsou výrazně procesně orientované aplikace. Zejména CEPR vede uživatele (soudce, vyššího

[61] Polčák, R. O dědovi Ministerstvu, babičce Justici a pračce ElectroJustici, *Jiné právo* [online], vydáno 11. 5. 2008 [cit. 13. 11. 2011]. Dotupné z: <http://jinepravo.blogspot.com/2008/05/o-ddoviministerstvu-babice-justici.html>.

soudního úředníka, asistenta soudce, soudního tajemníka) krok za krokem od příjmu podání, až po rozhodnutí ve věci samé a jeho doručení, a tyto kroky jsou napevno dány samotným informačním systémem. Pokud by chtěl uživatel učinit nějaký nestandartní úkon, který je však dle jeho názoru v rámci zákona možný, aplikace mu to neumožní.

Často se v odborných článcích na téma eJustice zmiňuje její hlavní nedostatek, a tím je absence elektronických soudních spisů. S tím je spojena nutnost tisknou elektronická podání a zakládat je do listinných spisů. Dle mého názoru je však třeba vše vnímat v širších souvislostech. Přestože počet podání v elektronické podobě neustále roste, i nadále převažují podání listinná. Pokud by se zavedly elektronické soudní spisy pro všechny agendy, je pravdou, že by orgány justice přestaly být „hromadnými tiskárnami“, ale místo toho by se staly „hromadnými skenery“, protože by listinná podání bylo nutné před založením do elektronického spisu naskenovat. Povinné zavedení elektronické komunikace s orgány justice ve všech agendách, které by tento problém vyřešilo, je dle mého názoru nyní utopie a narážela by právě na přístup k právu na soudní ochranu.

Někdy jsou zmiňovány jako řešení tzv. „hybridní spisy“, které by obsahovaly dokumenty jak listinné, tak i elektronické (podle toho jakým způsobem byly doručeny či byly vytvořeny na soudech). Zejména u rozsáhlejších spisů se však jedná opět o věc velice problematickou zejména z hlediska orientace ve spisu.

Další hrozbou spojenou s elektronickými spisy je možnost problémů s aktuální přístupností do obsahu spisů. Přestože např. aplikace CEPR běží souběžně na dvou serverech a jsou zde ještě další prvky ochrany, nebývají až tak výjimečné dočasné (někdy i hodinové) výpadky systému. Toto lze ovšem jen stěží tolerovat v agendách, kde soud nařizuje jednání. Představa, že bude soud přerušovat či odročovat jednání z důvodů výpadku elektronických spisů se jeví jako neudržitelná.

Je tedy potřeba pečlivě zvažovat a určit, kdy elektronizace justice, stejně jako celý eGovernment, ještě přináší pro organizace a uživatele přínos, a kdy už se jedná pouze o marné a nesmyslné pokusy. Je třeba přihlédnout dostupnosti k internetu, k počítačové gramotnosti obyvatelstva, ale i úředníků orgánů veřejné moci, včetně justice, tedy hlavně k tomu, zda jsou lidé ochotni a schopni využívat ještě ty které části e-Governmetnu.

Zavádění informačních systémů a jejich údržba jsou finančně značně nákladné. Na aktuálním příkladu justice je možno ukázat ještě další finanční riziko, a tím je četnost legislativních změn a s tím spojené požadavky na úpravu informačních systémů. Příkladem může být nový zákon o veřejných rejstřících, který zavedl nové rejstříky, jako spolkový rejstřík či rejstřík ústavů. To si vyžádalo nejen změnu tzv. inteligentních formulářů pro zasílání podání, ale rovněž rozsáhlou změnu celé aplikace ISVR.

4.3 Návrhy na zlepšení

V první fázi by dle mého názoru měla být vytvořena a schválena promyšlená a provázaná koncepce rozvoje eGovernmentu a eJustice. Rozvoj eGovernemtu by měl probíhat při průběžné konzultaci s odborníky na veřejnou správu, právníky a s odbornou veřejností. Dále by měla probíhat úzká spolupráce mezi jednotlivými ministerstvy při rozvoji eGovernemtu a předávání informací a zkušeností. Až po zvážení všech rizik a alternativ, lze dle mého mínění pokračovat v dalším zavádění eGovernmentu. Pro schválenou koncepci by měly být zajištěny dostatečné finanční prostředky pro její realizaci tak, aby nezůstala „na půli cesty“, což se stalo již pravidlem.

E-participaci lze v případě justice omezit prakticky pouze na poskytování informací o své činnosti. Domnívám se, že organizace justice by i přes zavedení aktivního poskytování dat o své činnosti prostřednictvím aplikací infoSoud, infoJednání, infoData a Judikatura mohly zlepšit způsob informování o své činnosti. Internetové stránky jednotlivých organizací jsou značně nepřehledné, údaje na nich jsou neaktuální a některé, pro veřejnost podstatné informace, zcela chybí. Dále informování účastníků řízení o průběhu řízení má dle mého názoru další možnosti rozvoje. Jedná se např. o možnost nahlížet do elektronických spisů vzdáleným přístupem, který v současné době i přes zavedení aplikace CEPR chybí. Co se týče poskytování informací pro účastníky řízení prostřednictvím telefonu (tzv. infocentra), tak zde rovněž chybí jednotný postup organizací justice. Rozsah poskytovaných informací se značně liší. Jako jednu z možností zpřístupnění údajů o řízení i pro účastníky řízení v řízeních, kde nejsou zavedeny spisy v elektronické podobě, bych viděl v generování a následném zasílání účastníkům přístupových hesel. Po jejich následném sdělení pracovníkovi infocentra by mohli být účastníku poskytnuty podrobnější informace o stavu jeho řízení.

Již jsem zmínil možnost nahrazení „dřevěných“ úředních desek informačními panely, na které by se z informačních systémů spisové služby přenášela rozhodnutí, výzvy a sdělení pro účastníky, a to bez nutnosti jejich tisku.

Z konkrétních kroků směřujících ke zlepšení komunikace občanů s orgány veřejné moci bych chtěl uvést ještě např. zavedení on-line placení správních a soudních poplatků. Měl by to být jednotný a zabezpečený systém pro celou oblast veřejné správy, který by umožnil činit platby např. s využitím platebních karet okamžitě při podání příslušného návrhu. K tomu by musela nutně přispět i legislativní opora, která by jednoznačně stanovila možnost takový způsob využívat a dále určila, maximální výši částky za platby odváděné provozovatelům platebních systémů.

Závěr

Práce si kladla za cíl provedení studie teoretického vymezení eGovernmentu v České republice a jeho následnou komparaci se skutečným fungováním na příkladu eJustice, která tvoří jeho důležitou součást. Smyslem nebylo pouze opisovat teoretické koncepty přístupu k elektronizaci veřejné správy. Cílem bylo ukázat skutečné problémy, které jsou s rozvojem eGovernmentu spojeny, a které nejsou dle mého názoru v žádné odborné literatuře popsány.

V první části byl obecně vymezen pojem eGovernmentu a různé pohledy na něj. Rovněž byl stručně popsán vývoj v České republice, jeho současné legislativní a institucionální zabezpečení. Ve druhé části byly deskribovány jednotlivé aktuální prvky eGovernentu.

Třetí část práce pak na základě znalostí, které jsem získal během své praxe u soudu a Ministerstva spravedlnosti ČR, byla vedena snahou o popis skutečné praxe a důsledků zavádění eGovernmentu. Cílem bylo popsat, jak jsou základní, legislativně upravené části eGovernmentu, využívány v justici, a co justice učinila či činí nad rámec zákonných povinností, a dále vzájemnou provázanost jednotlivých prvků eGovernemtu.

Čtvrtá část obsahuje zejména upozornění, že nelze jednoduše konstatovat, že eGovernment v České republice trpí základními nedostatky a nelze jej využívat, nebo naopak, že vše funguje naprosto bez problémů. Celý problém elektronizace veřejné správy je nesmírně složitý, justici nevyjímaje. Jedná se o neustále balancování mezi požadavky občanů na dobrou správu věcí veřejných a její transparentnost a mezi představami politiků a pracovníků veřejné správy, mezi rozvojem informačních technologií a mezi počítačovou gramotností osob, které veřejnou správu využívají, mezi omezenými finančními prostředky na rozvoj eGovernmentu a mezi přínosy elektronizace.

Seznam zkratek

G2G – government to government

G2B – government to business

G2C – government to ciziten

ISVS – informační systém veřejné správy

DS – datová schránka

ZR – základní registry

ISDS – informační systém datových schránek

o.s.ř. – občanský soudní řád

v.k.ř. - vnitřní a kancelářský řád

CEO – centrální evidence obyvatel

CIS – cizinecký informační systém

RZE – rejstřík zahájených exekucí

EŽOPEX – elektronická žádost o pověření exekuce

ISAS- informační systém administrativy soudů

ISVKS – informační systém vrchních a krajských soudů

ISIR - informační systém insolvenčního rejstříku

ISKS – informační systém krajských soudů

CEPR – centrální platební rozkaz

EPR – elektronický platební rozkaz

CESO – centrální evidence stíhaných osob

ISVR – informační systém veřejných rejstříků

ISNS – informační systém Nejvyššího soudu

Seznam použité literatury

Knižní zdroje:

1. MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2., podstatně přeprac. a rozš. vyd. Praha: Leges, 2012, 464 s. Teoretik. ISBN 978-80-87576-36-6.

2. HENDRYCH, Dušan. *Správní právo: obecná část*. 7. vyd. Praha: C.H. Beck, 2009, xxxviii, 837 s. Právnické učebnice (C.H. Beck). ISBN 978-807-4000-492.

3. POMAHAČ, Richard. *Základy teorie veřejné správy*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011, 267 s. ISBN 978-80-7380-330-8.

4. SMEJKAL, Vladimír a Michal Altair VALÁŠEK. *Jak na datové schránky: praktický manuál pro každého*. Praha: Linde, 2012, 197 s. ISBN 978-808-6131-801

5. ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. Vyd. 1. V Praze: C.H. Beck, 2012, xix, 258 s. Beckova edice ekonomie. ISBN 978-807-4002-618.

6. PELIKÁNOVÁ, Irena. *Obchodní právo*. Vyd. 1. Praha: ASPI, 2005, 458 s. ISBN 80-735-7062-9.

7. BUDIŠ, Petr a Iva HŘEBÍKOVÁ. *Datové schránky: fungování, doručování, bezpečnost, návody*. 1. vyd. Olomouc: ANAG, 2010, 287 p. ISBN 978-80-7263-617-4

8. ŠTĚDROŇ, Bohumír a Iva HŘEBÍKOVÁ. *Občanské soudní řízení sporné a využití informačních technologií a právních informačních systémů: (e-justice)*. 1. vyd. Praha: Linde, 2008, 271 s. ISBN 978-807-2017-140

9. LECHNER, Tomáš. *Elektronické dokumenty v právní praxi /: Tomáš Lechner*. Praha: Leges, 2013, 255 s. ISBN 978-80-87576-41-0.

10. PAVLÍČEK, Václav. *Ústavní právo a státověda*. Praha: Linde, 2004, 241 s. ISBN 80-720-1472-2.

11. SMEJKAL, Vladimír. *Datové schránky v právním řádu ČR: zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, s komentářem*. 1. vyd. Praha, 2009, 176 s. ISBN 978-80-86284-78-1.

12. WINTEROVÁ, Alena a Alena MACKOVÁ. *Civilní právo procesní: vysokoškolská učebnice*. 7. aktualiz. a dopl. vyd. Praha: Linde, 2014, 621 s. ISBN 978-807-2019-403.

Elektronické zdroje:

1. Ministerstvo vnitra. *Indikátory Prioritní osy 1a,1b: Oblasti intervence: 1.1A, 1.1B - Rozvoj informační společnosti ve veřejné správě* [online]. [cit. 2013-12-12]. Dostupné z: www.mvcr.cz/soubor/indikatory-prioritnich-os-1a-a-1b-pdf.aspx
2. Ministerstvo vnitra. *Efektivní veřejná správa a přátelské veřejné služby: Strategie realizace Smart Administration v období 2007 - 2015* [online]. 2007. vyd. 2007 [cit. 2013-12-19]. Dostupné z: www.mvcr.cz/soubor/modernizace-dokumenty-strategie-pdf.aspx
3. Peterka, J. Jak budou fungovat elektronické podpisy po 1. červenci? [online]. Vydáno 26. 5. 2012 [cit. 3. 2. 2014]. Dostupné z: < http://www.lupa.cz/clanky/jak-budou-fungovat-elektronicke-podpisy-po-1-cervenci/>
4. *Webový portál datových schránek* [online] [cit. 19. 3. 2014]. Dostupné z: < http://www.datoveschranky.info/cz/o-datovych-schrankach/slovnik-pojmu-id34696/>
5. Stanovisko Ministerstva vnitra [online]. Vydáno 15.9.2012 [cit. 1.3.2014]. Dostupné z: <http://www.mvcr.cz/clanek/stanovisko-k-problematice-udaju-umoznujicich-jednoznacnou-identifikaci-podepisujici-osoby.aspx>
6. PETERKA, Jiří a Jan PODANÝ. ASJA. [online]. [cit. 2014-10-20]. Dostupné z: http://asja.jacz.cz/index.php?pageid=1002&task=7&course_id=2477
7. *Webový portál OtevřenáData.cz* [online] [cit. 15. 10. 2014]. Dostupné z: < http://www.otevrenadata.cz/ otevrena-data /co-jsou-otevrena-data/>
8. Polčák, R. O dědovi Ministerstvu, babičce Justici a pračce ElectroJustici, *Jiné právo* [online], vydáno 11. 5. 2008 [cit. 13. 11. 2011]. Dotupné z: <http://jinepravo.blogspot.com/2008/05/o-ddoviministerstvu-babice-justici.html>.

Odborné články:

1. KORBEL, Fratišek. Elektronická spravedlnost (2). *Právo & Byznys*. 2012, 1/2012
2. KORBEL, Fratišek. Elektronická spravedlnost (1). *Právo & Byznys*. 2011, 12/2011
3. KORBEL, František a Prudíková DANA. Datové schránky tři roky poté: praktické zkušenosti s jejich používáním. *Bulletin advokacie*. 2012, roč. 2012, č. 5.

Legislativa

1. Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (zákon o archivnictví)
2. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
3. Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
4. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
5. Zákon č. 111/2009 Sb., o základních registrech
6. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
7. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
8. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
9. Zákon č. 99/1963 Sb., občanský soudní řád
10. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád),
11. Zákon č. 150/2002 Sb., soudní řád správní.
12. Zákon č. 500/2004 Sb. správní řád
13. Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
14. Vyhláška č. 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu)
15. Vyhláška č. 37/1992 Sb., o jednacím řádu pro okresní a krajské soudy
16. Instrukce Ministerstva spravedlnosti ze dne 3. prosince 2001, č.j. 505/2001-Org, kterou se vydává vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy
17. Instrukce č. 133/2012-OD-ST, kterou se upravuje jednotný postup podatelny při příjmu a ověřování datových zpráv a dokumentů v nich obsažených
18. Instrukce č. 20/2002-SM, ze dne 20.6.2002, kterou se upravuje postup při evidenci a zařazování rozhodnutí okresních, krajských a vrchních soudů do systému elektronické evidence soudní judikatury

Judikatura

1. Nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011
2. Rozsudek Nejvyššího správního soudu v rozhodnutí č. j. 8 As 89/2011 – 31 ze dne 17. 2. 2012
3. Nález Ústavního soudu sp. zn. II. ÚS 3042/12 ze dne 27. 8. 2013
4. Nález Ústavního soudu sp. zn. IV. ÚS 1829/13 ze dne 12. 2. 2014
5. Usnesení Vrchního soudu v Praze, č.j. 14 Cmo 114/2013-68, ze dne 25.3.2014

Seznam obrázků

Seznam tabulek

Abstract

Cílem práce je provedení studie teoretického vymezení eGovernmentu v České republice a jeho následnou komparaci se skutečným fungováním v praxi. Smyslem nebylo pouze opisovat teoretické koncepty přístupu k elektronizaci veřejné správy, ale ukázat skutečné problémy, které jsou s rozvojem eGovernmentu spojeny, a které nejsou dle mého názoru v žádné odborné literatuře popsány.

V první části byl obecně vymezen pojem eGovernmentu a různé pohledy na něj. Rovněž byl stručně popsán vývoj v České republice, jeho současné legislativní a institucionální zabezpečení. Ve druhé části byly deskribovány jednotlivé aktuální prvky eGovernentu.

Třetí část práce pak na základě znalostí, které jsem získal během své praxe u soudu a Ministerstva spravedlnosti ČR, byla vedena snahou o popis skutečné praxe a důsledků zavádění eGovernmentu. Cílem bylo popsat, jak jsou základní, legislativně upravené části eGovernmentu, využívány v justici, a co justice učinila či činí nad rámec zákonných povinností, a dále vzájemnou provázanost jednotlivých prvků eGovernmentu.

Čtvrtá část obsahuje zejména upozornění, že nelze jednoduše konstatovat, že eGovernment v České republice trpí základními nedostatky a nelze jej využívat, nebo naopak, že vše funguje naprosto bez problémů. Celý problém elektronizace veřejné správy je nesmírně složitý, justici nevyjímaje. Jedná se o neustále balancování mezi požadavky občanů na dobrou správu věcí veřejných a její transparentnost a mezi představami politiků a pracovníků veřejné správy, mezi rozvojem informačních technologií a mezi počítačovou gramotností osob, které veřejnou správu využívají, mezi omezenými finančními prostředky na rozvoj eGovernmentu a mezi přínosy, elektronizace.

Abstract

The aim of this work is to study the theoretical definition of e-Government in the Czech Republic and its subsequent comparison with the actual functioning in practice. The purpose was not only to describe the theoretical concepts and approaches to e-Government, but to show the real problems that are associated with the development of e-Government, and which are not, in my opinion, described in any scientific literature.

In the first part, the general definition and different views on eGovernment was described. Also its development in the Czech Republic was briefly mentioned, together with its current legislative and institutional background. The second part describes the actual individual elements of e-Government.

The third part of the work was based on the knowledge that I gained during my work at the court and Ministry of Justice. It was motivated by an effort to describe the actual practice and the consequences of the introduction of e-Government. The aim was to describe how are the basic, legislatively modified, parts of eGovernment used in the judiciary, and what has the judiciary made, or is making, beyond the legal obligations, and also to describe interdependence of the various elements of e-Government.

The fourth part contains mainly a notice that it can not be simplified that e-Government in the Czech Republic suffers from fundamental flaws and can not be used, or conversely, that everything works without any problems. The whole issue of electronisation of the public administration is extremely complex, including the judiciary. It is a constant balancing between the demands of citizens for good governance and its transparency and the ideas of politicians and civil servants, between the development of information technologies and computer literacy among the users o the public administration, between the limited financial resources on the development of e-Government and the benefits of computerization.

Název práce v anglickém jazyce

e-Government

Název práce v českém jazyce

e-Government

Klíčová slova v anglickém jazyce

e-Government, eJustice

Klíčová slova v českém jazyce

e-Government, eJustice

Seznam příloh:

Příloha č. 1 Právní předpisy upravující eGovernment a eJustici

1. **zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů** (dále jen zákon o archivnictví)

a) vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
b) vyhláška č. 654/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů

2. **zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů** (dále jen zákon o ISVS)

a) vyhláška č. 528/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému, který obsahuje základní informace o dostupnosti a obsahu zpřístupněných informačních systémů veřejné správy (vyhláška o informačním systému o informačních systémech veřejné správy)
b) vyhláška č. 53/2007 Sb., o technických a funkčních náležitostech uskutečňování vazeb mezi informačními systémy veřejné správy prostřednictvím referenčního rozhraní (vyhláška o referenčním rozhraní)
c) vyhláška č. 469/2006 Sb., formě a technických náležitostech předávání údajů do informačního systému o datových prvcích a o postupech Ministerstva informatiky a jiných orgánů veřejné správy při vedení, zápisu a vyhlašování datových prvků v informačním systému o datových prvcích (vyhláška o informačním systému o datových prvcích)
d) vyhláška č. 52/2007 Sb., o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb informačních systémů veřejné správy prostřednictvím referenčního rozhraní
e) vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení informačních systémů veřejné správy

3. **zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)** (dále jen zákon o elektronickém podpisu)

a) vyhláška č. 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného

elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu)

b) vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb)

4. **zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů** (dále jen zákon o DS)

a) vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů

b) vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek

5. **zákon č. 111/2009 Sb., o základních registrech** (dále jen zákon o ZR)

a) nařízení vlády č. 161/2011 Sb., o stanovení harmonogramu a technického způsobu provedení opatření podle § 64 až 68 zákona o základních registrech

b) vyhláška č. 359/2011 Sb., o základním registru územní identifikace, adres a nemovitostí

6. **Zákon č. 106/1999 Sb., o svobodném přístupu k informacím**

7. **Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů**

8. **Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)**

Vnitřní předpisy Ministerstva spravedlnosti upravující eJustici

- Vyhláška č. 37/1992 Sb., o jednacím řádu pro okresní a krajské soudy
- Instrukce 505/2001-Org, kterou se vydává vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy

- Pokyn obecné povahy nejvyššího státního zástupce poř. č. 7/2004, jímž se vydává kancelářský řád státního zastupitelství, ve znění pozdějších předpisů.
- Instrukci č. 133/2012-OD-ST, kterou se upravuje jednotný postup podatelny při příjmu a ověřování datových zpráv a dokumentů v nich obsažených
- Instrukce č. 20/2002-SM, ze dne 20.6.2002, kterou se upravuje postup při evidenci a zařazování rozhodnutí okresních, krajských a vrchních soudů do systému elektronické evidence soudní judikatury
- Instrukce Ministerstva spravedlnosti č. 26/2000-OI, kterou se stanoví postup pro předávání údajů obchodního rejstříku externím odběratelům
- Instrukce Ministerstva spravedlnosti č. 13/2002-OI-SP-2, o používání elektronického podpisu v resortu spravedlnosti.
- Instrukce Ministerstva spravedlnosti č. 95/2002-SOBŘ, o zabezpečení utajovaných skutečností zpracovávaných informačními systémy v resortu Ministerstva spravedlnosti
- Instrukce Ministerstva spravedlnosti č. 94/2007-OIS-ST, kterou se vydává skartační řád pro okresní, krajské a vrchní soudy, ve znění pozdějších předpisů.
- Instrukce Ministerstva spravedlnosti č. 157/2008-OD-ST, kterou se upravují povinnosti a postup při zveřejňování informací v aplikaci infoDeska resortu justice.

Příloha č. 2: Vzhled identifikátoru používaného v justici

Záznam o ověření elektronického podání doručeného na elektronickou podatelnu: Městský soud v Praze

dle vyhlášky 259/2012 Sb.

Pořadové číslo zprávy:	*61978 / 2014*	Ev. číslo:	*28ff195b-1fd6-4506-8baf-2ac3ccfdc72e*
Druh podání:	*Elektronická pošta*	ID zprávy:	
Věc:	*MSPH 96 INS 15017/2012 - DIOS Šternberk, s.r.o.*		
Odesílatel:			
ID schránky:		Typ datové schránky:	
Osoba:	***Pavla Kociánová***	Adresa:	*pavla.kocianova@cez.cz*
Doručeno do emailové schránky dne:		***01.04.2014 15:02:36***	
Č.j. příjemce:		Č.j. odesílatele:	
Sp.zn. příjemce:		Sp.zn. odesílatele:	
Lhůta končí:		K rukám:	*Ne*
Číslo zákona:	Paragraf v zákoně:	Odstavec paragrafu:	Písmeno v paragrafu:
Ověření obálky:	*Podpis je platný*		
Podepsal:	*Pavla Kociánová*	Vystavil:	*I.CA - Qualified Certification Authority, 09/2009*
Sériové číslo certifikátu:	*a67fd3*	Platnost:	*11.03.2014 - 11.03.2015*
Antivirový test:	*Proběhl v mailovém systému*	Obsah podání:	*OK*
Elektronický podpis:	*Platný*	Časové razítko:	*Nepřipojeno*
Certifikát:	*Ověřeno na základě CRL z 01.04.2014 13:52:12*		
Datum a čas autom. ověření:	*01.04.2014 15:17:09*		

Počet podaných příloh:7

Číslo přílohy Výsledek	Název příl. CRL	Identifikace podepisující osoby	Identifikace vystavitele certifikátu	T	U	K	P	R	A	C	V
1	*Přihláška DIOS Štemberk, s.r.o..pdf*										
Podpis je platný	*CRL z 01.04.2014 13:52:12*	*Pavla Kociánová / a67fd3 / 11.03.2014 - 11.03.2015*	*I.CA - Qualified Certification Autho...*	*A*	*A*	*N*	*	-	*A*	-	-
1.1	*VOPD.pdf*										
Podpis není připojen (žádný podpis).				*A*	*N*	*N*					
1.2	*4634789702.pdf*										
Značku nelze ověřit (certifikát vypršel)		*Autorizace tiskového výstupu / a2d91a / 26.10.2011 - 25.10.2012*	*I.CA - Qualified Certification Autho...*	*A*	*A*	*N*	*N*	-	*A*	-	-
1.3	*4634789791.pdf*										
Značku nelze ověřit (certifikát vypršel)		*Autorizace tiskového výstupu / a2d91a / 26.10.2011 - 25.10.2012*	*I.CA - Qualified Certification Autho...*	*A*	*A*	*N*	*N*	-	*A*	-	-
1.4	*Smlouva.pdf*										
Podpis není připojen (žádný podpis).				*A*	*N*	*N*					
1.5	*plná moc Kociánová Pavla.pdf*										
Podpis není připojen (žádný podpis).				*A*	*N*	*N*					
1.6	*výpis z OR ČEZ Prodej.pdf*										
Podpis není připojen (žádný podpis).				*A*	*N*	*N*					

Čas ověření příloh:	*01.04.2014 15:17:09*	Ověření příloh:	*ověřováno automaticky*

Vysvětlení stavů při ověření příloh (vztaženo vždy k datu a času dodání):

Stav "?" znamená, že systém tuto operaci ještě neprovedl, ale provedena bude

Stav "-" znamená, že systém tuto operaci neprovádí

Stav "!" znamená, že systém tuto operaci nemůže provést

Kontrola podpisů a razítek byla provedena na základě CRL seznamů platných k datu a času ověření datové zprávy.

Příloha č. 3: Postup podatelny při ověřování elektronických podpisů

1. Byla integrita dokumentu po podpisu změněna?
    a. Ano, vyhodnocení **Podpis je neplatný (dokument po podpisu byl změněn)**
    b. Ne, bod 2
2. Jedná se o kvalifikovaný certifikát?
    a. Ano, bod 3)
    b. Ne, vyhodnocení **Podpis není připojen (není uznávaný)**
3. Je certifikát platný časově (je v intervalu platnosti v okamžiku dodání do CEPO?)
    a. Ano, čeká se na CRL, bod 4)
    b. Ne, bod 5)
4. Je certifikát obsažen v prvním CRL vydaném po přijetí podání?
    a. Ano, bod 5)
    b. Ne, vyhodnocení **Podpis je platný**
5. Je přiloženo kvalifikované časové razítko a je neporušené?
    a. Ano, bod 6)
    b. Ne, vyhodnocení **Podpis je neplatný (certifikát vypršel)** nebo **Podpis je neplatný (certifikát byl zneplatněn)**
6. Je poslední přiložené časové razítko platné?
    a. Ano, bod 7)
    b. Ne, vyhodnocení **Podpis je neplatný (certifikát a časové razítko je neplatné)**
7. Bylo razítko přiloženo před koncem platnosti certifikátu?
    a. Ano, bod 9)
    b. Ne, bod 8)
8. Bylo zkoumané razítko přiloženo před koncem platnosti předchozího razítka?
    a. Ano, bod 7)
    b. Ne, vyhodnocení **Podpis je neplatný (certifikát vypršel)**
9. Existuje záznam o zneplatnění certifikátu?
    a. Ano, bod 10)
    b. Ne, vyhodnocení **Podpis je platný** (Platnost certifikátu prodloužena časovým razítkem)
10. Byl certifikát zneplatněn před vložením časového razítka?
    a. Ano, vyhodnocení **Podpis je neplatný (certifikát byl zneplatněn)**.
    b. Ne, vyhodnocení **Podpis je platný**